COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione n. 70 del 04/04/2025

Assessore Proponente: MONTAUTI DAVIDE

OGGETTO: APPROVAZIONE DEL PIANO DI PROTEZIONE DEI DATI PERSONALI E DI GESTIONE DEL RISCHIO DI VIOLAZIONE

L'anno duemilaventicinque addì quattro del mese di aprile alle ore 12:30 nella Casa Comunale, previa l'osservanza di tutte le formalità prescritte dalla vigente Legge Comunale e Provinciale, sono stati convocati oggi a seduta i componenti della Giunta Comunale, che nelle persone seguenti risultano presenti alla trattazione della proposta di deliberazione in oggetto:

MONTAUTI DAVIDE	SINDACO	Presente
PAOLINI CHIARA	VICE SINDACO	Assente
MAI DANIELE	ASSESSORE	Assente
LENZI STEFANO	ASSESSORE	Presente (Skype)
SPINETTI JACOPO	ASSESSORE	Presente (Skype)

Presenti n. 3 Assenti n. 2

Partecipa il SEGRETARIO ROSSI ANTONELLA che provvede alla redazione del presente verbale.
Presiede la seduta, nella sua qualità di SINDACO, il Sig. MONTAUTI DAVIDE che dichiara aperta la trattazione dell'oggetto sopra indicato.

Deliberazione n. 70 del 04/04/2025

copia informatica per consultazione

LA GIUNTA COMUNALE

Rilevato che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

Considerato che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

Tenuto presente che tale evoluzione ha indotto l'Unione europea ad adottare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

Dato atto che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

Rilevato che, con il GDPR, è stato richiesto agli Stati membri:

- un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

Richiamata la Legge 25 ottobre 2017, n. 163 e, in particolare, l'art. 13, che ha delegato il Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR;

Rilevato che il decreto legislativo delegato è finalizzato a realizzare l'adeguamento sulla base dei seguenti *principi e criteri direttivi* specifici:

a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;
b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;
c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

copia informatica per consultazione

d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;
e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse;

Ritenuto che l'adeguamento dell'ordinamento nazionale interno al GDPR renda necessario definire le politiche e gli obiettivi strategici da conseguire per garantire l'adeguamento;

Dato atto che, sulla base del delineato quadro normativo, l'obiettivo di fondo del GDPR è la sicurezza del trattamento dei dati personali, programmando e pianificando gli interventi affinché i dati personali siano:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatto salvo l'adeguamento di misure tecniche e organizzative adeguate richieste dal presente GDPR a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Ritenuto che l'obiettivo di assicurare la sicurezza dei dati richiede di gestire efficacemente, e conformemente alle disposizioni del GDPR, il rischio di violazione dei dati derivante dal trattamento, per tale dovendosi intendere la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e che, a tal fine, vadano definiti gli obiettivi correlati alla gestione del rischio;

Atteso che il paragrafo 5.5.3 della norma UNI ISO 31000 - Standard di gestione del rischio-, contiene l'indicazione di predisporre e di attuare *Piani di trattamento del rischio* e di documentare, secondo il *principio di tracciabilità documentale*, come le opzioni di trattamento individuate che sono state attuate;

copia informatica per consultazione

Valutata l'opportunità, pur non aderendo l'Ente al sistema volontario di certificazione UNI ISO 31000, di fare riferimento allo Standard internazionale per le attività relative alla gestione del rischio di violazione dei dati personali e nella predisposizione del Piano di Protezione Dati;

Ritenuto, pertanto, necessario procedere alla approvazione di un piano di protezione dei dati personali e di gestione del rischio di violazione;

Visto l'allegato schema di Piano;

Appurato che:

- la funzione principale dello stesso è quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale;
- il documento consente che la strategia si sviluppi e si modifichi in modo da mettere via via a punto degli strumenti di protezione mirati e sempre più incisivi;
- l'adozione del documento non si configura come un'attività una tantum, bensì come un processo continuo in cui le strategie e gli strumenti vengono via via affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione;
- eventuali aggiornamenti successivi, anche infra annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD, sono oggetto di approvazione da parte dello stesso organo che ha approvato il PPD;

Considerato che lo schema di Piano è stato predisposto dal responsabile del procedimento con il coinvolgimento e la partecipazione degli attori indicati nello Schema di Piano medesimo e, in particolare con la partecipazione dei dirigenti/responsabili P.O.;

Dato atto che, al fine di garantire il livello essenziale delle prestazioni, l'Amministrazione è tenuta a garantire la pubblicazione del presente provvedimento e dello schema di piano allegato sul sito web dell'Amministrazione, nella apposita sezione "Amministrazione trasparente" e nella sottosezione "Altri contenuti-anticorruzione";

Visti:

- D.Lgs. 267/2000;
- Legge 241/1990;
- D.Lgs. 196/2003;
- Legge 190/2012;
- D.Lgs. 33/2013;
- Regolamento (UE) n. 679/2016;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla *"portabilità dei dati"* - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento *"possa presentare un rischio elevato"* ai sensi

copia informatica per consultazione

del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Statuto Comunale;
- Regolamento di organizzazione degli uffici e dei servizi;
- Regolamento sul trattamento dei dati sensibili;
- Codice di comportamento interno dell'Ente;
- Circolari e direttive del RPC;

Acquisito il parere di regolarità tecnica ai sensi dell'art. 49 del Tuel e dando che la presente deliberazione non necessita del parere di regolarità contabile in quanto non comporta riflessi diretti o indiretti né sulla situazione economico-finanziaria né sul patrimonio dell'Ente

Ad unanimità di voti espressi nelle forme di legge

Delibera

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1. Di approvare l'allegato schema di Piano di protezione dei dati personali e di gestione del rischio di violazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016;

3. Di dare atto che il Piano è soggetto ad aggiornamento in correlazione agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD;

4. Di comunicare i contenuti del Piano a tutti i soggetti indicati nel Piano medesimo, attraverso i canali dallo stesso individuati, e di demandare ai dirigenti/responsabili P.O. nonché a tutti i dipendenti l'attuazione del Piano;

5. Di disporre che al presente provvedimento venga assicurata:
   a) la pubblicità legale con pubblicazione all'Albo Pretorio
      nonché
   b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "Amministrazione trasparente", sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali";

7. Di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.Lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di perti-

copia informatica per consultazione

nenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.

8. Di dichiarare, con separata ed unanime votazione, il presente provvedimento immediatamente eseguibile ai sensi dell'articolo 134, comma 4, del decreto legislativo 18 agosto 2000, n. 267, in ragione dell'esigenza di celerità correlate dei procedimenti amministrativi.

copia informatica per consultazione

COMUNE DI CAMPO NELL’ELBA
Provincia di Livorno
******

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

Verbale n. 16 del 04.04.2025

IL SINDACO
MONTAUTI DAVIDE

IL SEGRETARIO
ROSSI ANTONELLA

copia informatica per consultazione

Comune di CAMPO NELL'ELBA

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE[1]
per una gestione del rischio robusta

- approvato con Deliberazione di Giunta Comunale n. _____ del _____
e in adeguamento della norma UNI ISO 31000
e conforme al REGOLAMENTO UE 2016/679 -

1 Il paragrafo 5.5.3 della norma UNI ISO 31000 prevede la predisposizione e l'adeguamento di "PIANI DI TRATTAMENTO DEL RISCHIO" aventi lo scopo di documentare come le opzioni di trattamento scelte sono attuate e indica, altresì, le informazioni da fornire nei suddetti piani. L'Ente si è conformato alla norma esclusivamente per le attività relative alla gestione del rischio di violazione dei dati personali e nella predisposizione del presente Piano.

copia informatica per consultazione

Titolo del Documento Piano di protezione dei dati
Numero di versione: 01

Data ultimo aggiornamento: 06/03/2025

Stato del documento: Approvato dal Titolare del Trattamento

Estensori del documento: Titolare del Trattamento

Riferimento per comunicazioni in merito al documento: Comune di Campo nell'Elba - Email: -posta@comune.camponellelba.li.it - Pec: comune.camponellelba.li@postacert.toscana.it

Modalità di distribuzione del presente documento e delle eventuali nuove versioni: Pubblicato nella sezione "Privacy" di Amministrazione Trasparente del sito istituzionale.

copia informatica per consultazione

PREMESSA

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea ('Cartà) e l'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea ('TFUE') stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
Le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche. Senonché, la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali.

In adeguamento al GDPR (reg. UE 2016/679), il presente Piano di protezione dei dati personali (PPD) intende rappresentare lo strumento, il fulcro del sistema di protezione adottato dall'Ente.

copia informatica per consultazione

PARTE I
PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE (PPD)

DEFINIZIONI
Il presente documento recepisce e utilizza le seguenti definizioni:
- GDPR: il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR generale sulla protezione dei dati);

- 'WP29': gruppo di lavoro articolo 29 sulla protezione dei dati, per tale dovendosi intendere il Gruppo di lavoro istituito in virtù' dell'articolo 29 della direttiva 95/46/CE quale organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata con i suoi compiti fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE;

- 'PPD': il presente Piano di Protezione dei Dati personali e gestione del rischio di violazione;

- 'Regolamento dati sensibili': il Regolamento interno, approvato dal titolare in conformità allo schema tipo approvato dal Garante, che identifica e rende pubblici, per i trattamenti dei dati sensibili e giudiziari, i tipi di dati e le operazioni eseguibili;

- 'ID': identificativo.

OGGETTO
Il PPD individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà' fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle MISURE DI SICUREZZA informatiche/logiche, logistiche/fisiche, organizzative e procedurali da adottare e da applicare per ridurre/eliminare il RISCHIO di violazione dei dati derivante dal trattamento.
La disciplina si applica ai:

1.trattamenti con strumenti elettronici;

2.trattamenti senza l'ausilio di strumenti elettronici (ad esempio: cartacei, audio, visivi e audiovisivi, ecc.).

FINALITÀ
Il presente documento, in attuazione del GDPR e della normativa interna di adeguamento, e' funzionale alla protezione dei diritti e delle libertà' fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali trattati nell'esercizio dell'attività istituzionale in un quadro di garanzie per gli interessati che contempla nuovi diritti. Sul presupposto che costituisce un OBIETTIVO STRATEGICO la sicurezza del trattamento dei dati personali, scopo del presente documento è programmare e pianificare gli interventi affinché i dati personali siano trattati conformemente ai principi dell'art. 5 del GDPR.

QUADRO NORMATIVO DI RIFERIMENTO
Il PPD tiene conto dei seguenti documenti:
- Codice in materia di dati personali (D.Lgs. n.196/2003);

- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

- D.Lgs. n. 101/2018 di adeguamento della normativa interna al GDPR;

- Dichiarazioni e Linee Guida del gruppo di lavoro articolo 29;

copia informatica per consultazione

- Regolamenti interni, approvati dai titolari e/o dai responsabili.

ATTORI INTERNI ALL'AMMINISTRAZIONE CHE HANNO PARTECIPATO ALLA PREDISPOSIZIONE DEL PIANO, NONCHE' CANALI E STRUMENTI DI PARTECIPAZIONE
Oltre al titolare, hanno contribuito alla predisposizione del Piano, per quanto di propria competenza:

- dirigenti/responsabili E.Q. delegati al trattamento e, loro tramite, gli incaricati del trattamento in relazione,

- responsabile Protezione dei dati - RPD.

CANALI, STRUMENTI E INIZIATIVE DI COMUNICAZIONE DEI CONTENUTI
Il Piano viene portato alla conoscenza dei dipendenti, dei collaboratori, della cittadinanza e dei soggetti a qualunque titolo coinvolti nell'attività dell'ente mediante i seguenti strumenti:
- pubblicazione sul sito istituzionale a tempo indeterminato sino a revoca o sostituzione con un PPD aggiornato;

- invio a tutto il personale dipendente tramite rete intranet e all'OIV.

copia informatica per consultazione

PARTE II
DATI PERSONALI, RISCHIO DI VIOLAZIONE E DISCIPLINA DEL GDPR

IL RISCHIO PER I DIRITTI E LE LIBERTÀ' DEGLI INTERESSATI E LA NEUTRALIZZAZIONE DEL RISCHIO ATTRAVERSO IL SISTEMA DI PROTEZIONE BASATO SU UNI ISO 31000

Nell'attuale contesto, lo sviluppo e la rapidità dell'evoluzione tecnologica nonché la globalizzazione comportano nuove sfide per la protezione dei dati personali. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. Nel contempo, la tecnologia attuale consente a soggetti pubblici e privati di utilizzare dati personali come mai in precedenza, e la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati, tenuto conto dell'aumento del rischio di violazione dei dati medesimi e della necessità che le persone fisiche abbiano il controllo dei dati personali che li riguardano in un quadro di certezza giuridica e operativa rafforzata così come delineata del GDPR.
Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà' e sui diritti degli interessati.

Rispetto a tali possibili impatti negativi, il titolare del trattamento è tenuto a promuovere e adottare approcci e politiche che tengano conto costantemente del rischio, effettuando una analisi attraverso un apposito processo di valutazione (si vedano artt. 35-36 GDPR) che sappia tenere conto:

- dei rischi noti o evidenziabili;

- delle misure tecniche e organizzative adottate o che si intende adottare per mitigare il rischio.

All'esito dell'analisi, condotta anche attraverso la valutazione di impatto (DPIA), il titolare del trattamento decide, in autonomia, se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale, fermo restando che l'autorità non ha il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e può ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58 GDPR (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

LA DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE

Le diverse componenti del sistema di protezione sono documentati almeno da:

- Piano protezione dati -PPD;

- Registri delle attività e delle categorie dei trattamenti;

- Mappa struttura organizzativa;

- Mappa dei soggetti;

- Mappa dei luoghi;

- Schede di ricognizione dei trattamenti/Indice-Mappa dei trattamenti;

- Mappa hardware;

- Mappa software;

- Mappa rischi e motivazioni stima;

copia informatica per consultazione

- Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679/ Schede di assoggettabilità a DPIA;

- Schede di valutazione di impatto (DPIA) per i trattamenti a rischio elevato;

- Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente;

- Mappa delle misure di sicurezza logistiche/fisiche;

- Mappa delle misure di sicurezza informatiche/logiche;

- Mappa delle misure di sicurezza organizzative;

- Mappa delle misure di sicurezza e procedurali;

- Elenco delle misure di sicurezza correlate all'indice dei trattamenti e suddivise per uffici.

GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000

Principi applicabili alla gestione del rischio

Sulla base della Norma UNI ISO 31.000, e ai fini della strategia di protezione dei dati personali, viene definita:

- la nozione di "rischio" come uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.

- la nozione di "gestione dei rischi" come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta tenendo presente i principi contenuti nella della Norma UNI ISO 31.000.

La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta attraverso le fasi di:

- analisi del rischio, quale fase del processo di gestione nella quale viene definito il contesto esterno e interno, di natura organizzativa e gestionale;

- valutazione del rischio, quale fase del processo di gestione del rischio che identifica, analizza e pondera il rischio medesimo;

- trattamento del rischio.

GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA ANALISI

Contesto interno organizzativo

L'articolo 35 del GDPR fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche".

Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "diritti e libertà'" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà' di parola, la libertà' di pensiero, la libertà' di circolazione, il divieto di discriminazione, il diritto alla libertà' di coscienza e di religione.

copia informatica per consultazione

I documenti allegati e, in particolare, la ricognizione dei trattamenti in rapporto a tutta l'attività dell'ente, le schede di DPIA e l'elenco dei rischi, della gravità rilevata dalla prospettiva degli interessati e della relativa motivazione comprovano l'effettuazione della analisi dei rischi derivanti dai trattamenti, e l'accuratezza della analisi medesima.

Contesto interno organizzativo

Struttura organizzativa

La struttura organizzativa dell'Ente e' indicata nella MAPPA DELLA STRUTTURA ORGANIZZATIVA allegata, e corrisponde alle funzioni istituzionali e ai compiti assegnati a ciascuna struttura.

La MAPPA DEI LUOGHI indica:

- la sede principale, con l'indicazione degli Uffici e la relativa descrizione;

- le sedi secondarie, con l'indicazione degli Uffici e la relativa descrizione.

Soggetti: Titolare del trattamento

Denominazione: Comune di Campo nell'Elba

Sede: Piazza Dante Alighieri n. 1

Punti di contatto: Email: posta@comune.camponellelba.li.it - Pec: comune.camponellelba.li@postacert.toscana.it

Il titolare del trattamento, sopra citato, esercita le funzioni e i compiti e assume le responsabilità indicate nel GDPR e della normativa interna di recepimento.

Soggetti: Contitolari del trattamento

La MAPPA DEI SOGGETTI, allegata al presente documento, riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, i casi in cui il titolare, sopra indicato, e uno o più altri titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

I contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente GDPR, con particolare riguardo:

- all'esercizio dei diritti dell'interessato;

- alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

Tale accordo deve designare un punto di contatto per gli interessati.

Soggetti: Responsabili del trattamento e sub-responsabili

La MAPPA dei soggetti, allegata al presente documento, riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, i casi in cui un trattamento debba essere effettuato per conto del titolare del trattamento, da un responsabile del trattamento che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

copia informatica per consultazione

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Soggetti: Incaricati

La MAPPA dei soggetti, allegata al presente documento, riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, l'Elenco dei casi in cui un il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali può trattare tali dati previa istruzione.

Contesto interno gestionale e operativo
L'Ente ha adottato, in adeguamento del D.Lgs. 30 giugno 2003, n. 196, il GDPR per il trattamento dei dati sensibili e giudiziari che identifica i tipi di dati sensibili e giudiziari e le operazioni eseguibili nello svolgimento delle proprie funzioni istituzionali con definizione dell'Indice dei trattamenti. I Dirigenti/Responsabili E.Q. ed incaricati hanno debitamente sottoscritto gli atti di designazione al trattamento dei dati ove sono richiamati i principi relativi al trattamento di dati sensibili e giudiziari nel previsti dal GDPR.

Schede di ricognizione dei trattamenti

Fanno parte del sistema di protezione le Schede di ricognizione dei trattamenti elaborate con riferimento a tutta l'attività svolta dall'Ente, prendendo in considerazione tutti i processi, inclusi i procedimenti amministrativi.

Mappa hardware

La Mappa hardware, allegata al presente documento per formarne parte integrante e sostanziale, identifica gli strumenti, i tipi di supporto e i locali di ubicazione. Fornisce, altresì, una descrizione delle caratteristiche tecniche degli strumenti elettronici medesimi.

Mappa software

La Mappa software, allegata al presente documento per formarne parte integrante e sostanziale, identifica i software in relazione agli archivi/banche dati che vengono gestiti dai software medesimi.

Identifica, altresì, i soggetti abilitati all'accesso.

Mappa dei rischi

La Mappa dei rischi, allegata al presente documento per formarne parte integrante sostanziale, costituisce un elenco dei principali eventi rischiosi che possono determinare la violazione dei dati e rileva, dalla prospettiva degli interessati, la gravità e la correlata motivazione.

Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679

Fanno parte del sistema di protezione le Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679, le quali vengono allegate al presente documento per formarne parte integrante sostanziale.

copia informatica per consultazione

Schede di valutazione di impatto sulla protezione dei dati (DPIA)

Fanno parte del sistema di protezione le Schede di valutazione di impatto sulla protezione dei dati (DPIA) che esaminano i trattamenti che presentano rischi elevati, le quali vengono allegate al presente documento per formarne parte integrante sostanziale.

Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) per la pubblicazione

Fanno parte del sistema di protezione le Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente.

Mappa misure di sicurezza logistiche/fisiche

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza logistiche/fisiche.

Mappa misure di sicurezza informatiche/logiche

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza informatiche/logiche.

Mappa misure di sicurezza organizzative

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza organizzative.

Mappa misure di sicurezza procedurali

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza procedurali.

Elenco misure di sicurezza

Fa parte integrante e sostanziale del sistema di protezione l'allegato ELENCO misure di sicurezza, correlate alla ricognizione/indice dei trattamenti e suddivise per uffici.

Registro delle attività di trattamento e delle categorie di attività

Fanno parte integrante sostanziale del sistema di protezione:

- il Registro delle attività ' di trattamento svolte sotto la responsabilità del titolare;

- il Registro del responsabile del trattamento contenente tutte le categorie di attività relative al trattamento svolte per conto del titolare.

Altri documenti del Sistema di protezione

Costituiscono parte del sistema di protezione, per formarne parte integrante sostanziale:

- atti di delega al trattamento dei dati;

- atti di nomina degli incaricati.

copia informatica per consultazione

Costituiscono parte del sistema di protezione, quand'anche non fisicamente allegati al presente documento, i seguenti ulteriori documenti:

- elenco misure minime ITC e relative implementazioni, adottato entro il 31 dicembre 2017;

- GDPR sulla protezione dei dati laddove approvato;

- piano di formazione in materia di diritti e di libertà' delle persone e di protezione dei dati personali per i soggetti autorizzati al trattamento e per incaricati del back up;

- contratti/clausole contrattuali con i responsabili del trattamento;

- pareri del Responsabile protezione dati;

- verbali di vigilanza del responsabile protezione dati;

- circolari;

- informazioni fornite al pubblico e agli interessati;

- altra documentazione utile a comprovare la conformità dei trattamenti al GDPR e alla normativa interna di adeguamento.

Contesto esterno: trattamenti affidati in outsourcing o effettuati da responsabili esterni
L'Elenco trattamenti affidati in outsourcing o comunque effettuati da responsabili esterni, e allegato al presente documento per formarne parte integrante sostanziale, consente di rilevare il rischio derivante dai trattamenti effettuate, nel contesto esterno alla struttura organizzativa del titolare.

copia informatica per consultazione

PARTE II
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA VALUTAZIONE

Determinazione di assoggettabilità dei trattamenti a valutazione di impatto – DPIA
In base alla Norma UNI ISO 31.000, la valutazione del rischio richiede l'identificazione, l'analisi e la ponderazione del rischio medesimo.

Ai fini della valutazione del rischio, il GDPR introduce l'obbligo di valutazione d'impatto del trattamento sulla protezione dei dati.

Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà' delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del GDPR.

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology (modello COBITS) nonché degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del GDPR:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà' degli interessati di cui al paragrafo 1, art. 35 del GDPR;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Rischi residui e consultazione Autorità di controllo
E' nei casi in cui il titolare del trattamento non riesca a trattare in maniera sufficiente i rischi individuati (ossia i rischi residui rimangono elevati) che questi deve consultare l'autorità di controllo.

Un esempio di un rischio residuo elevato inaccettabile include casi in cui gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio: accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad esempio: poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilità ben nota).

copia informatica per consultazione

PARTE III
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000 : FASE DEL TRATTAMENTO

Misure di sicurezza del trattamento
Il GDPR prevede che il titolare del trattamento attui misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto GDPR, tenendo conto tra l'altro dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà' delle persone fisiche" (articolo 24, paragrafo 1). L'obbligo per il titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 della presente Sezione.

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non e' istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Misure di sicurezza logistiche/fisiche
Sicurezza di aree e locali

L'identificazione delle misure di sicurezza logistiche/fisiche deve tenere conto almeno dei sotto indicati elementi di rischio, indicati a titolo esemplificativo e non esaustivo:

a) Collocazione

- Zona sismica

- Corsi d'acqua nelle vicinanze con rischio esondazione

- Aziende vicine con lavorazioni pericolose

- Installazioni vicine pericolose (aeroporti, depositi carburanti...)

- Area degradata

b) Vicinanza servizi

- Carabinieri o altre forze di polizia e vigilanza

- Ospedali o altri presidi

- Vigili del fuoco

c) Misure presenti antintrusione

- Antifurto

- Vigilanza

- Videosorveglianza

copia informatica per consultazione

- Controllo accessi

- Recinzioni

- Cancelli

d) Misure presenti antincendio

- Estintori

- Idranti

- Rilevatori

d) Misure presenti per la regolarità degli impianti

- Elettrico

- Climatizzazione

- Riscaldamento

e) Misure presenti per la continuità elettrica

- UPS

- Generatori

f) Procedure

- Procedura di gestione degli accessi

- Procedura di gestione dei visitatori/manutentori

L'identificazione delle misure di sicurezza logistiche/fisiche prende in considerazione almeno le principali sotto indicate misure, elencate a titolo esemplificativo e non esaustivo:

a) antifurto

- Sensori

- Allarmi

- Connessione con le forze dell'ordine

- Connessione con servizi di vigilanza

- Videosorveglianza

- Porta normale

- Porta blindata

- Serratura di sicurezza

- Finestre con grate

copia informatica per consultazione

- Finestre senza grate

b) antincendio

- Sensori

- Allarmi

- Estintori/Impianto antincendio

- Impianti a norma

- Porta taglia fuoco

- Porta antincendio per fuga

- Utilizzo materiale ignifugo

c) Sicurezza ambientale

- Piano di emergenza per la gestione dei rischi individuati

d) Sicurezza accessi

- Controllo

- Registrazione

- Altro

e) Sicurezza CED

- Adeguato posizionamento all'interno dell'edificio

- Adeguate pareti soffitto/pavimento

- Misure anti effrazione

- Controllo accessi

- Impianto di climatizzazione

- Misure antincendio idonee all'uso con le apparecchiature presenti

- Porte antincendio di adeguata dimensione

- Rilevatori di fumo, calore, allagamento

f) continuità operativa

- Gruppo di continuità

- Gruppo elettrogeno

- Coerenza fra i dispositivi di continuità e le normative VVFF

- Pavimento galleggiante per l'adeguato posizionamento dei cavi

copia informatica per consultazione

- Corretto ed ordinato posizionamento dei cavi elettrici

- Corretto ed ordinato posizionamento dei cavi di rete

- Posizionamento ordinato delle apparecchiature nei rack

- Spazio intorno ai rack adeguato per la movimentazione e manutenzione delle apparecchiature

g) Sistema di custodia archivi cartacei

- Armadi blindati

- Armadi ignifughi con serratura

- Armadi ignifughi senza serratura

- Altri armadi con serratura

- Altri armadi senza serratura

- Classificatori/cassetti con serratura

- Classificatori/cassetti senza serratura

- Cassaforte

- Scaffalature

La MAPPA delle misure di sicurezza logistiche/fisiche applicate i diversi trattamenti, allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Misure di sicurezza informatiche/logiche
Al fine di indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate per contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi, ed in adeguamento della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, AgID ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".

Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1 agosto 2015)", le Misure minime sono ora divenute di obbligatoria adozione per tutte le Amministrazioni.

L'adeguamento dell'Ente alle Misure minime è avvenuto entro il 31 dicembre 2017, come da documentazione in atti che si allega al presente piano per farne parte integrante e sostanziale.

Le Misure, che si articolano sull'adeguamento di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di adeguamento. Il livello minimo è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

Fra le misure minime è previsto anche:

copia informatica per consultazione

- che le pubbliche amministrazioni accedano sistematicamente a servizi di early warning che consentano loro di rimanere aggiornati sulle nuove vulnerabilità di sicurezza. A tal proposito il CERT-PA fornisce servizi proattivi ed informativi a tutte le amministrazioni accreditate.

Per l'identificazione delle misure minime informatiche/logiche, per la sicurezza ICT ai fini del presente PPD si rinvia alle suddette misure minime per la sicurezza ICT delle pubbliche amministrazioni come attuate e implementate dal titolare.

La MAPPA delle misure di sicurezza logistiche/fisiche applicate i diversi trattamenti inclusi i criteri e modalità di salvataggio e di ripristino della disponibilità dei dati, allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Misure di sicurezza organizzative
A titolo esemplificativo e non esaustivo, le misure di sicurezza organizzative fanno riferimento

a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati;

b) alle istruzioni da impartire agli incaricati medesimi;

c) al controllo, alla custodia e restituzione della documentazione;

d) al controllo degli accessi degli archivi/banche dati;

e) all’esercizio dei diritti favorendo l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati e garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati;

f) alla formazione di tutti i soggetti che trattano dati personali sotto l'autorità del titolare e del responsabile del trattamento, con divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'unione o degli stati membri;

g) alla gestione dei dati attraverso la distruzione dei documenti non necessari, alla separazione dei documenti e dati, alla utilizzazione adeguata dei documenti, ed attraverso misure necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del garante;

h) all’informazione continua ed aggiornamento costante su procedure operative e istruzioni;

i) alle prescrizioni soprattutto nell'attività di videosorveglianza del rispetto di tutte le misure e gli accorgimenti prescritti dall’autorità Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello";

l) ai trattamenti senza l'uso di strumenti elettronici garantendo l’aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative.

La MAPPA delle misure di sicurezza organizzative, applicate i diversi trattamenti allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Misure di sicurezza procedurali
Le misure di sicurezza organizzative sono identificate in base ai contenuti e indicazioni del GDPR.

A titolo esemplificativo e non esaustivo, si elencano di seguito alcune procedure possibili da definire ed attuare

copia informatica per consultazione

- definizione e attuazione procedura operativa per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati";

- definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante";

- definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico";

- definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali";

- definizione e attuazione procedura operativa per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati";

- definizione e attuazione procedura operativa per modalità di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 2015";

- definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia:

a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

b) le misure di ripristino in caso di "data breach";

- definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003 per i trattamenti con strumenti diversi da quelli elettronici:

a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati;

b) le modalità e i contenuti delle istruzioni da impartire agli incaricati medesimi;

c) le modalità del controllo, custodia e restituzione della documentazione;

d) le modalità del controllo degli accessi agli archivi/banche dati";

- definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonché per documentare i provvedimenti adottati per porvi rimedio nonché per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi";

- definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà' delle persone fisiche e sulla protezione di tali diritti e libertà', con particolare riferimento al diritto alla protezione dei dati personali b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del GDPR".

La MAPPA delle misure di sicurezza procedurali, applicate ai diversi trattamenti è allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Piano formativo
Il piano formativo deve essere impostato sulla di Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà' delle persone fisiche e sulla protezione di tali diritti e libertà', con particolare riferimento al diritto alla protezione dei dati personali.

copia informatica per consultazione

Notifica di una violazione dei dati personali all'Autorità di controllo

Per le notifiche all'Autorità di controllo, il presente PPD rinvia alla definizione e attuazione di adeguate misure organizzative e procedurali, ferma restando la disciplina del GDPR.

Comunicazione di una violazione dei dati personali all'interessato

Per la comunicazione di una violazione dei dati personali all'interessato, il presente PPD rinvia alla definizione e attuazione di adeguate misure organizzative e procedurali, ferma restando la disciplina del GDPR.

copia informatica per consultazione

ALLEGATI

01 - MAPPA STRUTTURA ORGANIZZATIVA ED ELENCO SOGGETTI INTERNI ED ESTERNI

02 - SCHEDE DI RICOGNIZIONE TRATTAMENTI ED ELENCO TRATTAMENTI E SCHEDE DPIA

03 - MAPPA DEI LUOGHI

04 - MAPPA HARDWARE

05 - MAPPA RISCHI E MOTIVAZIONI DI STIMA

06.1 - MAPPA MISURE D I SICUREZZA

06.2 – DELIBERAZIONE DI GIUNTA COMUNALE N. 39 DEL 07.03.2025 “APPROVAZIONE DOCUMENTO AGGIORNATO “MISURE MINIME DI SICUREZZA ICT” DI CUI ALLA CIRCOLARE AGID 2/2017”

07 - PROGRAMMAZIONE CORSI DI FORMAZIONE

20

copia informatica per consultazione

SERVIZIO	delegato interno	incaricato	contitolare	responsabile esterno
AREA Finanziaria e Tributaria (Servizio Finanziario - Servizio Bilancio - Ufficio Gestione Economica del Personale Dipendente - Servizio Economato - Servizio Tributi - Servizio Attività Economiche)	Dott. Servidei Stefano	Sig. Baldetti Giancarlo - Sig. Cottone Benedetto - Sig. Ferrini Giampiero - Sig.ra Ferrini Francesca - Dr.ssa Mattera Paola - Sig. Pacciardi Gabriele - Sig. Signorini Roberto		Banca Monte dei Paschi di Siena S.p.A - Consulente del lavoro Girardo Gabriella -PUBLISERVIZI SRL - I.C.A. - Imposte Comunali Affini S.p.A. - ETRURIA P.A. SPA - ApK srl
AREA TECNICA Lavori Pubblici e Ambiente (Servizio Lavori Pubblici - Gestione Patrimonio Immobiliare - Servizio Ambiente e Infrastrutture)	Arch. Braccesi Priscilla	Sig. Corsi Francesco - Sig. Cavicchioli Gaetano - Dott. Dini Carlo - Sig. Pisani Yuri - Sig. Piacentini Simone - Sig. Troccolo Luigi - Sig. Segnini Stefano - Sig. Costa Rolando - Sig. Montauti Paolo - Sig. Tesei Armando - Sig. Mazzei Emanuele		S.O.S. AMBIENTE Societa' tra Professionisti S.r.l - Elio watt srl - Retiambiente S.p.a.
AREA VIGILANZA (Servizio Polizia Urbana - Servizio Polizia Ammistrativa - Servizio di Protezione Civile)	Dott. Modica Di Marco Francesco	Sig. Munno Cesare - Sig. Orzati Massimiliano - Sig. Pietro Cottone - Sig.ra Lupi Claudia - Sig.ra Giovani Luciana - Sig.ra Oblato Lara - Sig.ra Martorella Chiara - Sig. Gentini Gian Mario		Fabio Pierulivo Impianti Elettrici e televisivi - Abaco SpA - STS srl - Maggioli Informatica SpA
AREA SEGRETARIO GENERALE (Segretario Comunale - Consiglio comunale e Commissioni Consiliari - Giunta Comunale - Sindaco - Attività Trasversali)	Dott.ssa Rossi Antonella			
AREA TECNICA EDILIZIA PRIVATA, URBANISTICA, DEMANIO (Servizio Edilizia - Servizio Urbanistica - Servizio Demanio)	Arch. Lancioni Silvia	Sig. Gelsi Simone - Sig. Testi Massimiliano - Sig. Tegas Iron		
Area Amministrativa (Servizio Segreteria Sindaco e Relazioni Esterne - Anagrafe - Stato Civile - Elettorale - Leva - Statistica e Polizia Mortuaria - Servizi Legali - Servizio Scuola e Biblioteca - Servizio Socio Culturale, Sport e Volontariato - Servizio Segreteria e Protocollo - Servizio Notifica - Ufficio Gestione Giuridica del Personale Dipendente)	Dott.ssa Mazzanti Agnese	Sig. Sergio Santinelli - Sig. Danesi Sauro - Sig. Mancini Alberto - Sig.ra Raino' Chiara - Sig.ra Rossi Carla - Dott. Tacchella Stefano - Sig.ra Fiorino Gabriella - Dott.ssa Galli M. Cristina - Sig.ra Avellino Virginia - Dott.ssa Peria Gloria - Dott.ssa Segnini Marina - Sig.ra Gargiulo Michela	Gestione associata archivi storici - Comune Marciana - Gestione associata archivi storici - Comune di Portoferraio - Gestione associata archivi storici - Comune di Rio - Gestione associata archivi storici - Comune di Porto Azzurro - Gestione associata archivi storici - Comune di Capoliveri - Gestione associata archivi storici - Comune di Marciana Marina - Istituto Comprensivo G. Giusti - Scuola Dell'Infanzia V.T. Battaglini - Sistema Documentario Territoriale Livornese - A.S.A. S.P.A. AZIENDA SERVIZI AMBIENTALI S.P.A. - ANCI - SGATE -	Arnera Societa' Cooperativa - Pelagos Societa' Cooperativa Sociale C.I.S.S.E. - Aquavision Servizi Marittimi S.r.l. - Ringest srl -Etruria p.a. S.r.l. - Cooperativa Italiana di Ristorazione s.c. - LINC scs - Itaca Societa' Cooperativa a.r.l. - Cooperativa Sociale Arca - Azienda USL Toscana Nord Ovest - Cooperativa Sociale C.I.S.S.E. - Soc. Coop. Soc. Europa Servizi; Infoelba s.r.l. - Elba Informatica s.a.s. - Apkappa s.r.l. - Next Step Solution s.r.l. - Datagraph s.r.l. - Maggioli S.p.A.

copia informatica per consultazione

AREA	SERVIZIO	SERVIZIO	n. processi	Responsabile
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	14	
	GIUNTA COMUNALE	Giunta comunale	21	
	SINDACO	Sindaco	8	
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	12	
02 - Area Amministrativi	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	73	
	SERVIZI LEGALI	Servizi Legali	4	
	SERVIZIO NOTIFICA	Servizio Notifica	3	
	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	11	
	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	58	
	SERVIZIO SEGRETERIA E PROTOCOLLO	Servizio Segreteria e Protocollo	10	
	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	39	
	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	36	
03 - AREA FINANZIARIA - TRIBUTARIA	Servizi Finanziari	Servizi Finanziari	3	
	Servizio Attivita' Economiche S.U.A.P.	Servizio Attivita' Economiche	1	
	Servizio Bilancio	Servizio Bilancio	21	
	Servizio Economato	Servizio Economato	3	
	Servizio Tributi	Servizio Tributi	9	
	Ufficio Gestione economica Personale	Ufficio Gestione economica del personale dipendente	1	
04 - Area tecnica Edilizia e Urbanistica	Servizio Demanio	Servizio Demanio	2	
	Servizio Edilizia	Servizio Edilizia	10	
	Servizio Urbanistica	Servizio Urbanistica	4	
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	13	
	Servizio Ambiente e Infrastrutture	Servizio Ambiente e Infrastrutture	6	
	Servizio Lavori pubblici	Servizio Lavori Pubblici	11	
06 - Area di Vigilanza	Servizio di Protezione Civile	Servizio di Protezione Civile	1	
	Servizio Polizia amministrativa	Servizio Polizia Ammistrativa	5	
	Servizio polizia urbana	Servizio Polizia Urbana	4	
07 - Attivita' Trasversali	Attivita' Trasversali	Attivita' Trasversali	1	

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

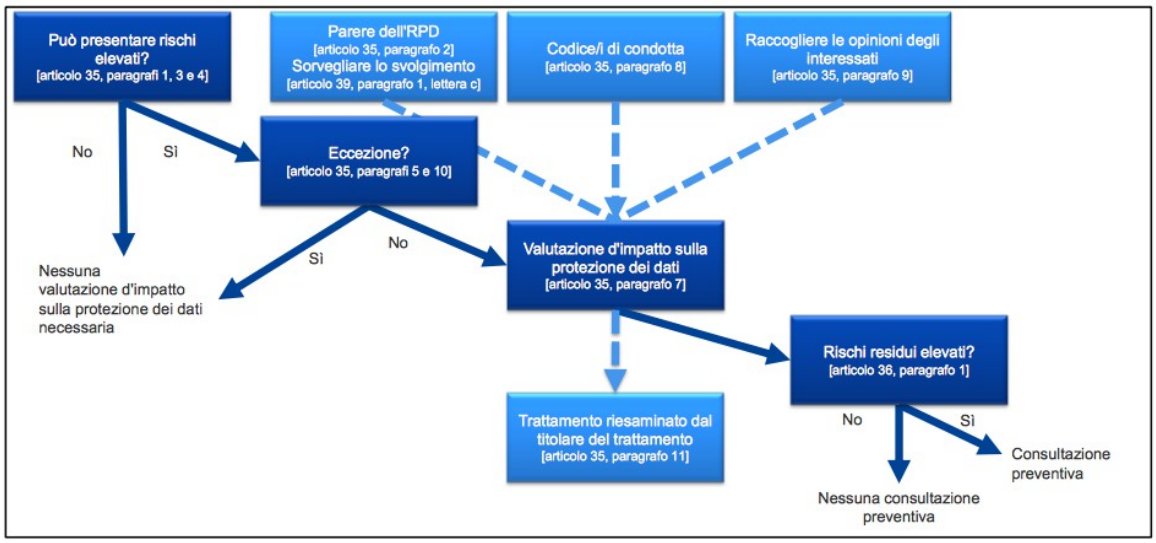
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

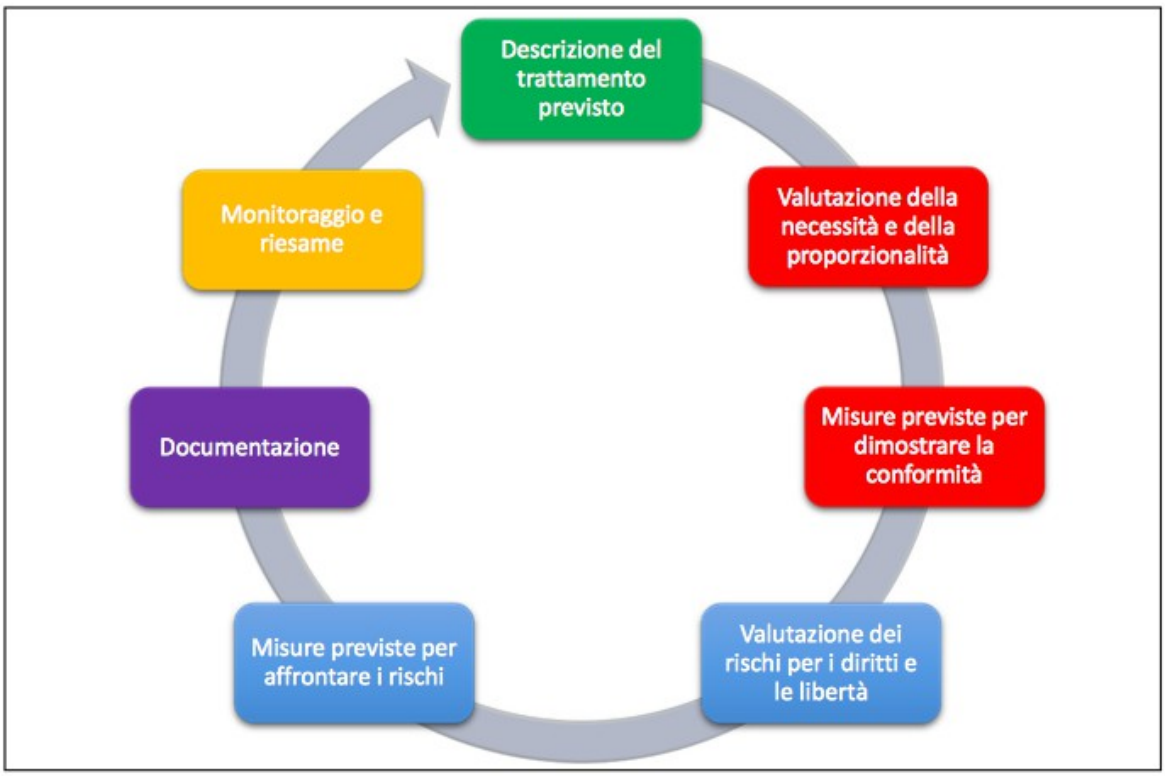
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Etruria p.a. S.r.l.
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 04 - Indipendentemente dall'alto numero di dati contenuti negli archivi anagrafici, quelli di carattere "sensibile" sono quelli concernenti l'origine razziale, in quanto tali idonei a rivelare le convinzioni religiose, inseriti negli anni 1938-44 in virtu' delle "leggi razziali"; questi dati, che sono idonei a rivelare in taluni casi anche le convinzioni religiose, non sono comunque resi noti (art. 3, r.d.l. n. 25/1944); ulteriori informazioni sull'origine razziale o etnica possono essere desunte dagli atti relativi alle adozioni internazionali. Altri dati sensibili contenuti in tali archivi possono essere raccolti anche da terzi e comunicati all'Autorita' giudiziaria per le cause di interdizione e decesso, alla ASL per l'aggiornamento del registro delle cause di morte. Vengono altresi' trattati dati di carattere giudiziario; le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 04 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (artt. 84 e ss.; artt. 106 e ss.; artt. 423 - 430) - L. 14.04.1982, n. 164 - D.P.R. 3.11.2000, n. 396 - D.P.R. 10.09.1990, n. 285
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 04 - Sistema informativo relativo all'attivita' di gestione dei registri di stato civile - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rivelare la vita sessuale (soltanto in caso di eventuale rettificazione di attribuzione di sesso) - Dati idonei a rivelare l'origine razziale (iscrizioni avvenute negli anni 1938-44) - Dati idonei a rilevare le convinzioni religiose (iscrizioni avvenute negli anni 1938-44)
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 04 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: Anagrafe, stato civile e servizio elettorale. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa

copia informatica per consultazione

	regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 04 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonche' rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalita' ai sensi dell'art. 2-sexies, comma 2 lett. b) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (atti e dei registri dello stato civile)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 04 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) ASL (per l'aggiornamento del registro delle cause di morte)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento*	

copia informatica per consultazione

effettuato tramite un sito web- Paese/i di ubicazione del/i server	
Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto

copia informatica per consultazione

Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Obbligo di inserire in ogni file oggetto di pubblicazione sui siti web istituzionali, potendo essere letto in un altro ambito e in un momento successivo alla sua diffusione, dei 'dati di contesto' (es. data di aggiornamento, periodo di validita', amministrazione, segnatura di protocollo o dell'albo), per liminare o ridurre il rischio di cancellazioni, modifiche, alterazioni o decontestualizzazioni - Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati

copia informatica per consultazione

	- Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Molto alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - livello dell'impatto, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Registro convivenze di fatto
Anagrafe: Iscrizioni registri anagrafici
Anagrafe: Cancellazioni registri anagrafici per irreperibilita'
Stato civile: Acquisizione della cittadinanza italiana per riconoscimento o dichiarazione giudiziale della filiazione durante la minore eta' del figlio, o nel caso in cui la paternita' o maternita' non puo' essere dichiarata, purche' sia stato riconosciuto giudizialmente il diritto al mantenimento o agli alimenti, di minore straniero
Stato civile: Acquisizione della cittadinanza italiana per riconoscimento o dichiarazione giudiziale della filiazione o nel caso in cui la paternita' o maternita' non puo' essere dichiarata, purche' sia stato riconosciuto giudizialmente il diritto al mantenimento o agli alimenti, di maggiorenne straniero
Anagrafe: Adeguamento anagrafe ai risultati del censimento
Toponomastica: Attribuzione numero civico
Toponomastica: Denominazione nuove strade e piazze
Anagrafe: Variazione di indirizzo
Stato civile: Tutela/Curatela
Stato civile: Trascrizione atti di nascita formati all'estero
Stato civile: Trasmissioni alla Procura della Repubblica
Stato civile: Comunicazioni all'Ufficio anagrafe
Stato civile: Celebrazioni matrimoni e unioni civili
Stato civile: Pubblicazioni di matrimonio
Stato civile: Disconoscimenti
Stato civile: Riconoscimenti
Stato civile: Annotazione sentenza di rettificazione attribuzione di sesso
Stato civile: Annotazione sentenze di scioglimento del matrimonio civile, di cessazione degli effetti civili del matrimonio religioso (concordatario) o di delibazione sentenze ecclesiastiche di annullamento di matrimonio pronunciate in Italia, provenienti da altri comuni
Separazione consensuale, divorzio congiunto e modifica delle condizioni di separazione o di divorzio innanzi all'Ufficiale di Stato Civile
Stato Civile: Trascrizione atto di matrimonio celebrato all'estero
Stato civile: Adozione
Stato civile: Trascrizione atti di nascita rese dalla Direzione Sanitaria
Atti di nascita, morte, cittadinanza e matrimonio
Stato civile: Trascrizione atto di nascita neo-cittadino
Stato civile: Trascrizione atto di matrimonio celebrato in altro comune italiano
Stato Civile: Trascrizione atto di matrimonio concordatario
Stato civile: Redazione atto di morte
Stato civile: Trascrizione atto di morte avvenuta all'estero
Stato civile: Trascrizione atto di morte pervenuto da altro Comune
Stato Civile: Rilascio passaporto mortuario
Pratiche anagrafiche

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

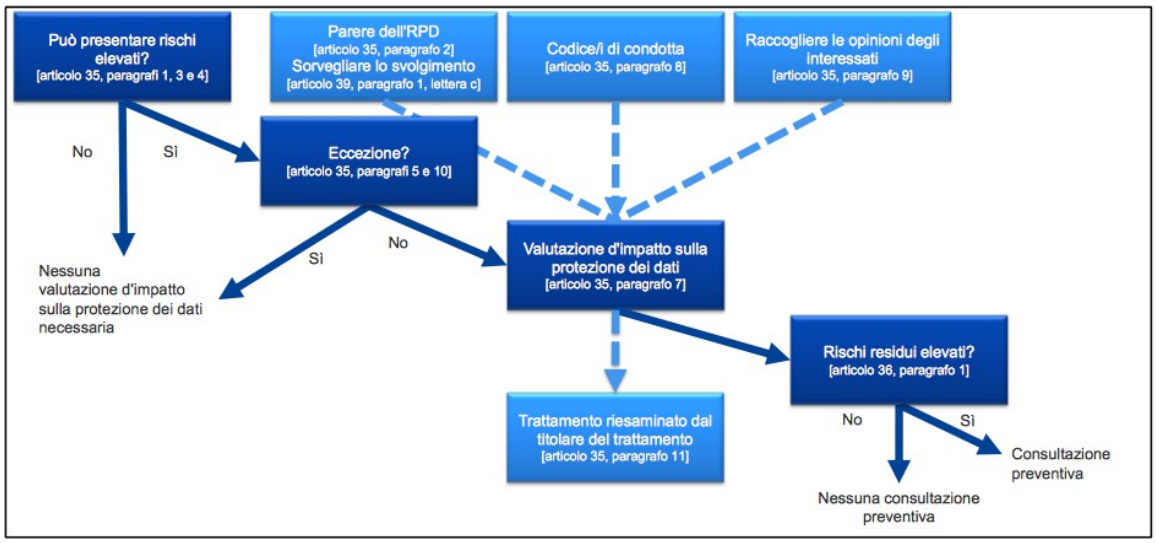
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

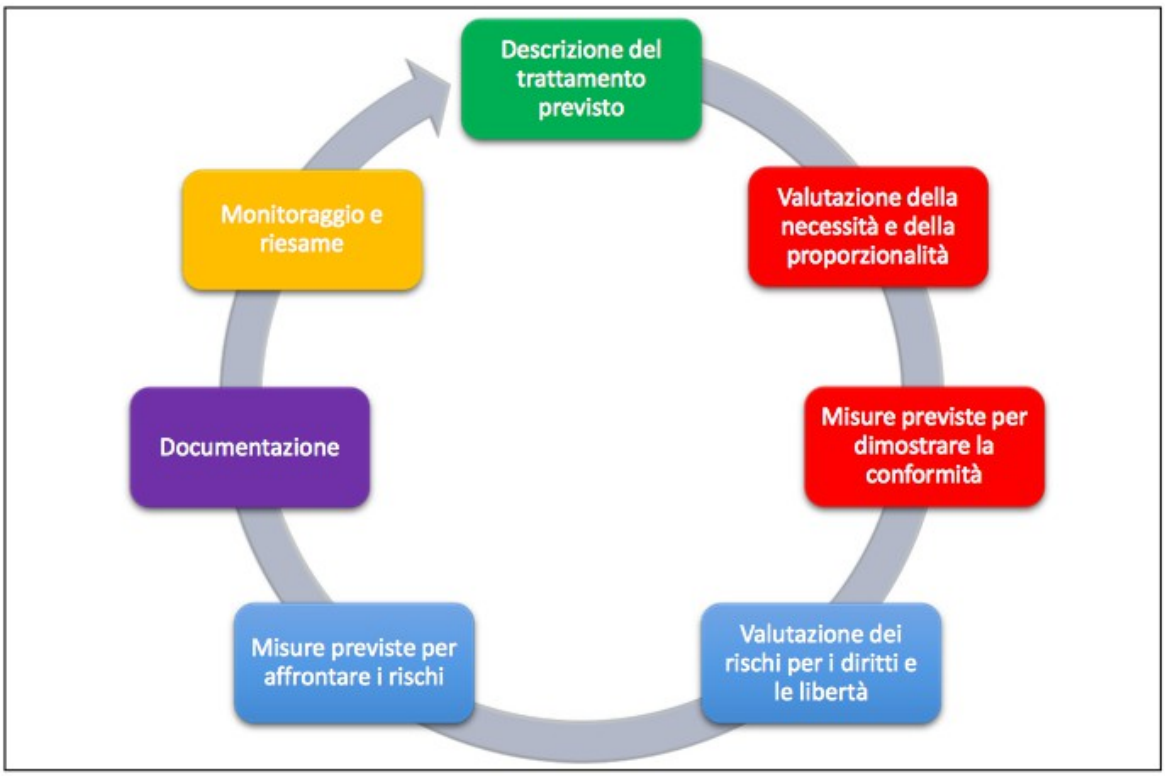
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 05 - Il procedimento finalizzato all'iscrizione nelle liste elettorali di chi abbia acquistato la residenza nel Comune inizia con la comunicazione, da parte dell'Ufficio Anagrafe, dell'avvenuta iscrizione di un cittadino nel registro della popolazione residente o nell'AIRE (anagrafe degli italiani residenti all'estero), ovvero con la rilevazione periodica dei cittadini che compiranno la maggiore eta' nel semestre successivo. L'eventuale esistenza di cause ostative di carattere giudiziario viene comunicata dal Comune di precedente residenza, che trasmette il fascicolo personale del cittadino trasferito o, per i residenti che acquisteranno la maggiore eta', viene accertata attraverso la certificazione appositamente richiesta al Casellario giudiziale. I predetti dati vengono altresi' comunicati alla Commissione elettorale circondariale al fine di aggiornare gli elenchi per la revisione semestrale delle liste elettorali. Coloro che non sono mai stati iscritti nelle liste elettorali o ne sono stati cancellati per cause ostative vengono iscritti o reiscritti d'ufficio al termine del periodo di incapacita'. Per coloro che sono gia' iscritti nelle liste elettorali, le comunicazioni riguardanti provvedimenti che possono determinare la perdita del diritto elettorale pervengono dall'Autorita' giudiziaria, dalla Questura o dall'Ufficio Territoriale del Governo. I dati sulla salute sono trattati al fine di permettere ai soggetti disabili di esercitare il proprio diritto di voto; mentre quelli religiosi rilevano in quanto nel territorio, nel quale esercitano il loro ufficio, gli ecclesiastici ed i ministri di culto, che hanno giurisdizione e cura di anime e coloro che ne fanno ordinariamente le veci; non possono ricoprire cariche elettive (art. 60 d.lg. n. 267/2000)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 05 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.P.R. 20.03.1967, n. 223 - L. 5.05.1992, n. 104 - D.Lgs. 18.08.2000, n. 267
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 05 - Sistema informativo relativo all'attivita' relativa all'elettorato attivo e passivo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare lo stato di salute: patologie attuali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 05 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: Anagrafe, stato civile e servizio elettorale. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione

copia informatica per consultazione

	europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 05 - Trattamento effettuato per rilevanti finalita' di interesse pubblico relative nella seguente materia: degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonche' rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalita' ai sensi dell'art. 2-sexies, comma 2 lett. b) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (liste elettorali e gestione delle consultazioni elettorali)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 05 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Commissione elettorale circondariale (per l'eventuale cancellazione dagli elenchi per la revisione semestrale delle liste elettorali dei cittadini che non siano in possesso dei requisiti per ottenere l'iscrizione nelle liste elettorali ai sensi del d.P.R. n. 223/1967)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): in caso di acquisto o riacquisto del diritto elettorale per cessazione di cause ostative, la deliberazione della Commissione elettorale comunale, unitamente all'elenco degli elettori iscritti ed alla relativa documentazione, viene depositata nella Segreteria del Comune (o presso l'Ufficio elettorale) nei primi cinque giorni del mese successivo ed ogni cittadino puo' prenderne visione (art. 32, comma 6, del d.P.R. n. 223/1967). Sono inoltre depositati per dieci giorni nell'Ufficio Elettorale gli atti relativi alla revisione semestrale delle liste elettorali ed ogni cittadino ha diritto di prenderne visione: tali atti possono riguardare provvedimenti dell'autorita' giudiziaria adottati nei confronti di minori che non vengono proposti per l'iscrizione (art. 18, comma 2, del d.P.R. n. 223/1967)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite*	

copia informatica per consultazione

un sito web-nome del dominio del sito web	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Commissione elettorale - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente

copia informatica per consultazione

	regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di

copia informatica per consultazione

	necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati* (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi

copia informatica per consultazione

	di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5

copia informatica per consultazione

	(CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti

copia informatica per consultazione

	- CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto	

copia informatica per consultazione

	con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita

copia informatica per consultazione

	l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di

copia informatica per consultazione

	ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Elettorale: supporto commissioni elettorali
Leva: Variazioni liste di leva
Elettorale: autorizzazione al voto fuori sezione
Elettorale: voto domiciliare
Gestione della leva
Elettorale: voto assistito
Elettorale: rilascio tessera elettorale
Elettorale: revisione dinamica liste elettorali

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

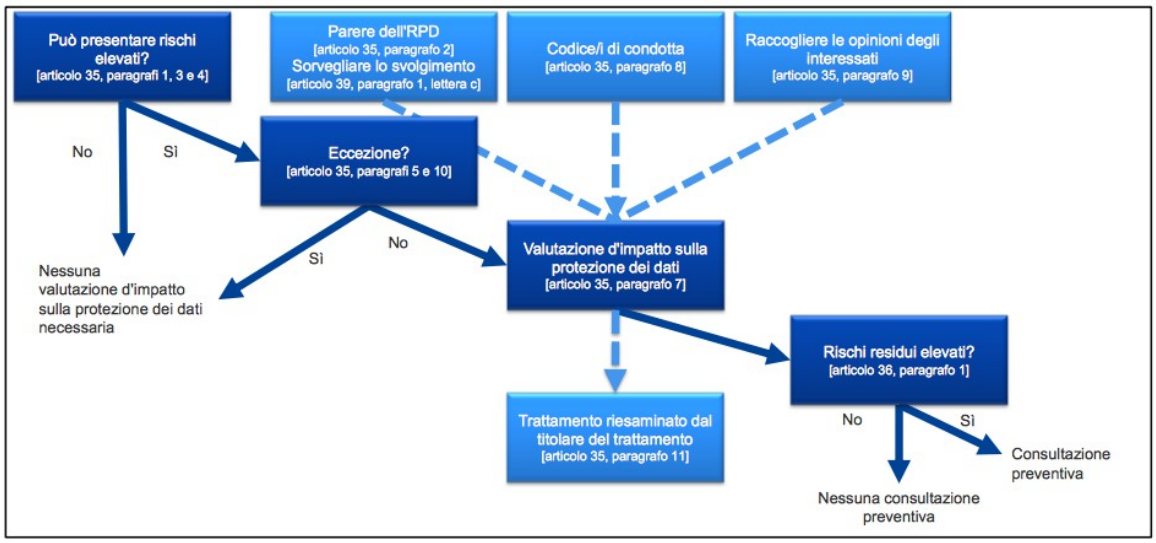
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

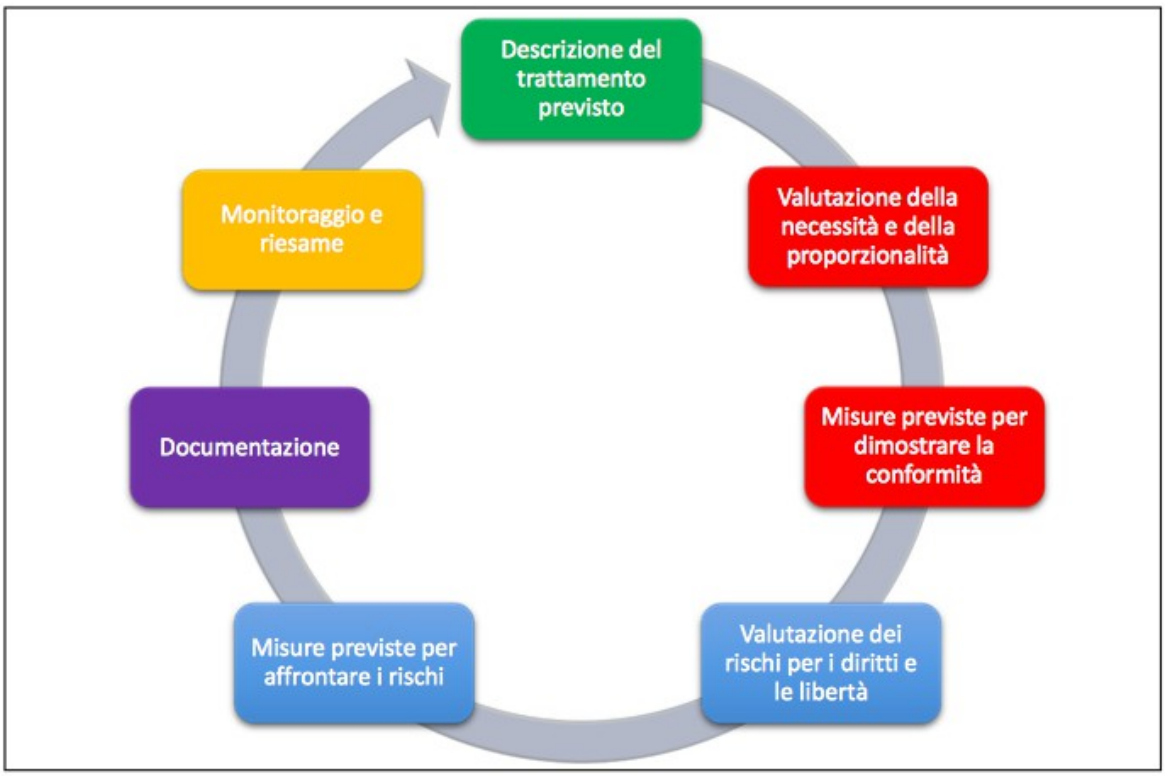
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 06 - I dati vengono forniti dall'interessato; la commissione elettorale comunale procede ad un'estrazione pubblica dei componenti del seggio; vengono confrontati con le liste di leva per la verifica del diritto al voto; vengono stampate le notifiche per gli scrutatori e redatti i verbali delle nomine. I dati sulla salute si riferiscono esclusivamente a quelli rinvenibili nei certificati medici che gli scrutatori sono tenuti a presentare in caso di indisponibilita' per motivi di salute.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 06 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 -

copia informatica per consultazione

	D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.P.R. 20.03.1967, n. 223 - L. 21.03.1990, n. 53 (presidenti) - L. 30.04.1999, n. 120 (scrutatori)
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 06 - Sistema informativo relativo alla tenuta degli Albi degli scrutatori e dei presidenti di seggio - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 06 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: Anagrafe, stato civile e servizio elettorale. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 06 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonche' rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalita' ai sensi dell'art. 2-sexies, comma 2 lett. b) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (svolgimento delle consultazioni elettorali; richieste di referendum, relative consultazioni e verifica della regolarita')
Interesse	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche,

copia informatica per consultazione

legittimo perseguito	nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Candidati a scrutatori o presidenti di seggio
Categorie di destinatari	- Nessun destinatario per le categorie particolari di dati
Strumenti e	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare,

copia informatica per consultazione

risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione

copia informatica per consultazione

Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a

copia informatica per consultazione

	trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

copia informatica per consultazione

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

copia informatica per consultazione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale

copia informatica per consultazione

	Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati)

copia informatica per consultazione

accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

copia informatica per consultazione

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative	

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni

copia informatica per consultazione

	del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio	- Rischio residuo non elevato, e conseguente decisione di procedere con il

copia informatica per consultazione

dopo l'applicazione delle misure	trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**

copia informatica per consultazione

art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Elettorale: iscrizione nell'albo degli scrutatori
Elettorale: aggiornamento Albo scrutatori
Gestione dell'elettorato
Elettorale: iscrizione nell'albo dei Presidenti di seggio

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

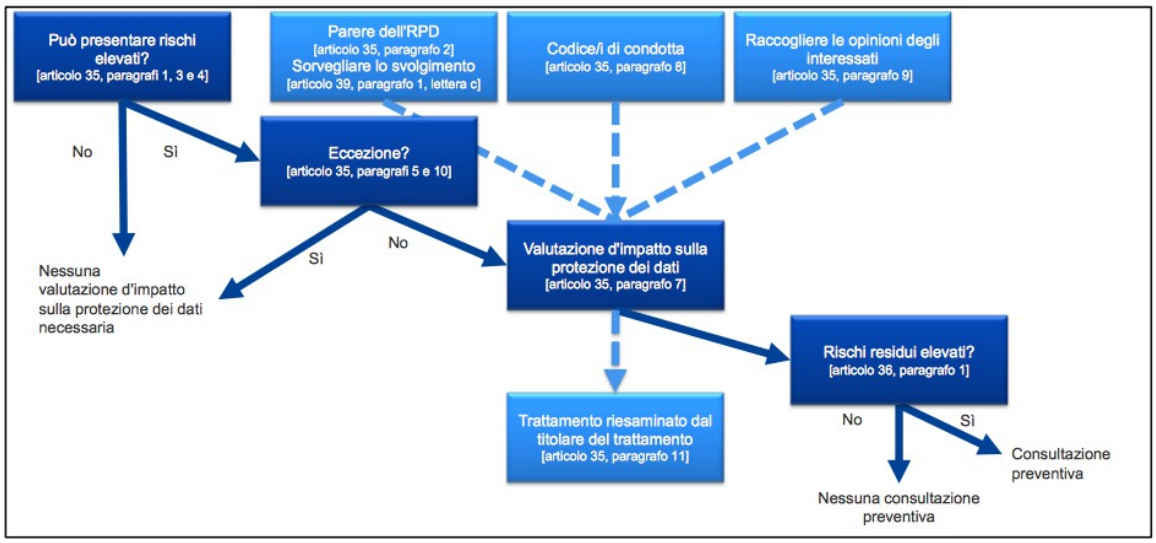
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

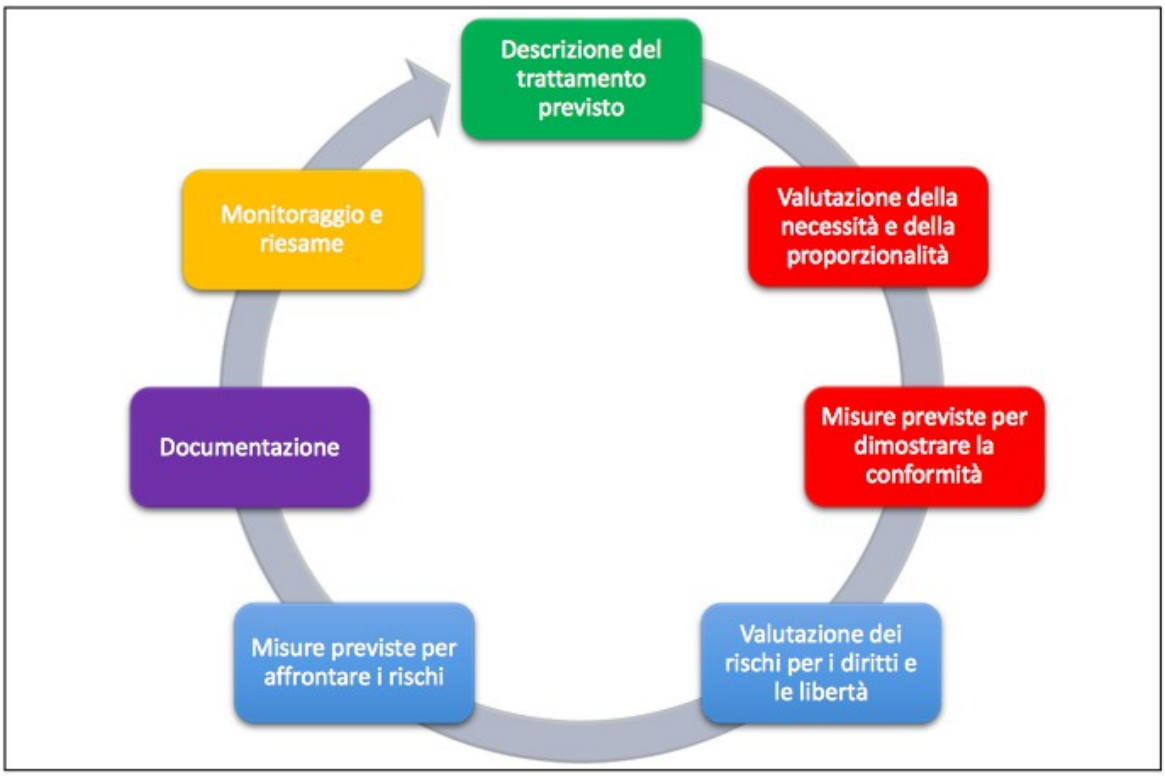
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 07 - I dati vengono forniti dall'interessato, che presenta una domanda contenente il titolo di studio e la professione, oppure vengono estratti casualmente dalle liste elettorali; vengono controllati i requisiti prescritti dalla legge e richieste le certificazioni necessarie anche a terzi. Viene quindi formato l'elenco provvisorio che e' trasmesso al Tribunale; quest'ultimo procede ad una verifica sui carichi pendenti e restituisce l'elenco al Comune per la pubblicazione e la formazione dell'elenco definitivo.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 07 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 -

copia informatica per consultazione

	D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 10.04.1951, n. 287 (elenchi dei giudici popolari)
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 07 - Sistema informativo relativo all'attivita' relativa alla tenuta dell'elenco dei giudici popolari - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003)
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 07 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: Anagrafe, stato civile e servizio elettorale. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 07 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonche' rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalita' ai sensi dell'art. 2-sexies, comma 2 lett. b) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' dirette alla tenuta degli elenchi dei giudici popolari)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una

copia informatica per consultazione

	delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 07 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Tribunale competente per territorio (per effettuare la verifica delle condizioni richieste dalla legge)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Iscritti o candidati alla iscrizione nelle liste dei giudici popolari
Categorie di destinatari	- Tribunale competente per territorio (per effettuare la verifica delle condizioni richieste dalla legge) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di

copia informatica per consultazione

	responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione

copia informatica per consultazione

Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a

copia informatica per consultazione

	trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

copia informatica per consultazione

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

copia informatica per consultazione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale

copia informatica per consultazione

	Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati)

copia informatica per consultazione

accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

copia informatica per consultazione

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative	

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni

copia informatica per consultazione

	del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio	- Rischio residuo non elevato, e conseguente decisione di procedere con il

copia informatica per consultazione

dopo l'applicazione delle misure	trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**

copia informatica per consultazione

art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Consultazioni elettorali
Elettorale: iscrizione nell'albo dei Giudici Popolari

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 09 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

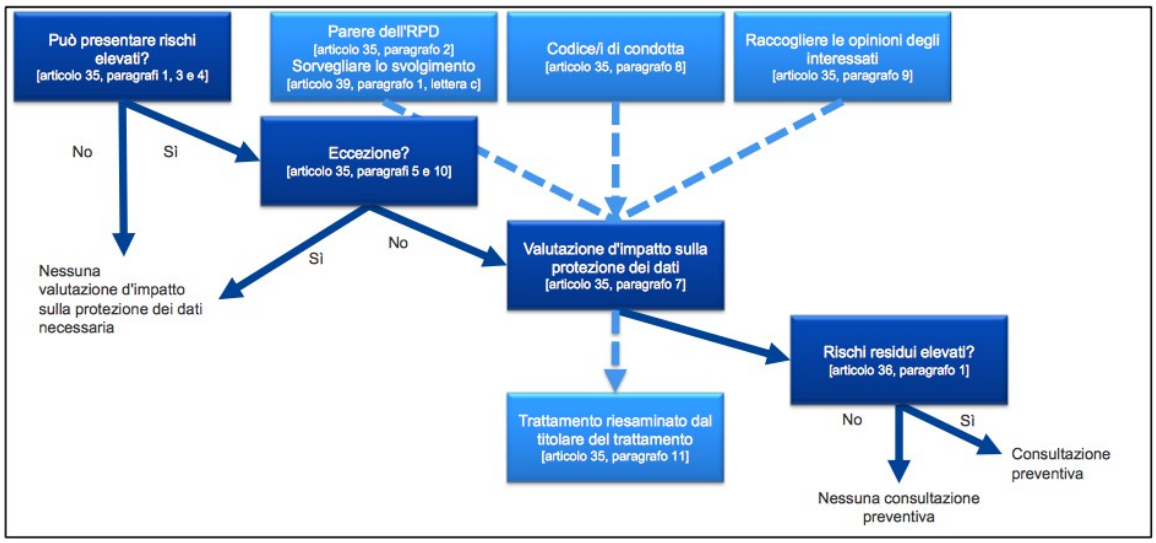
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

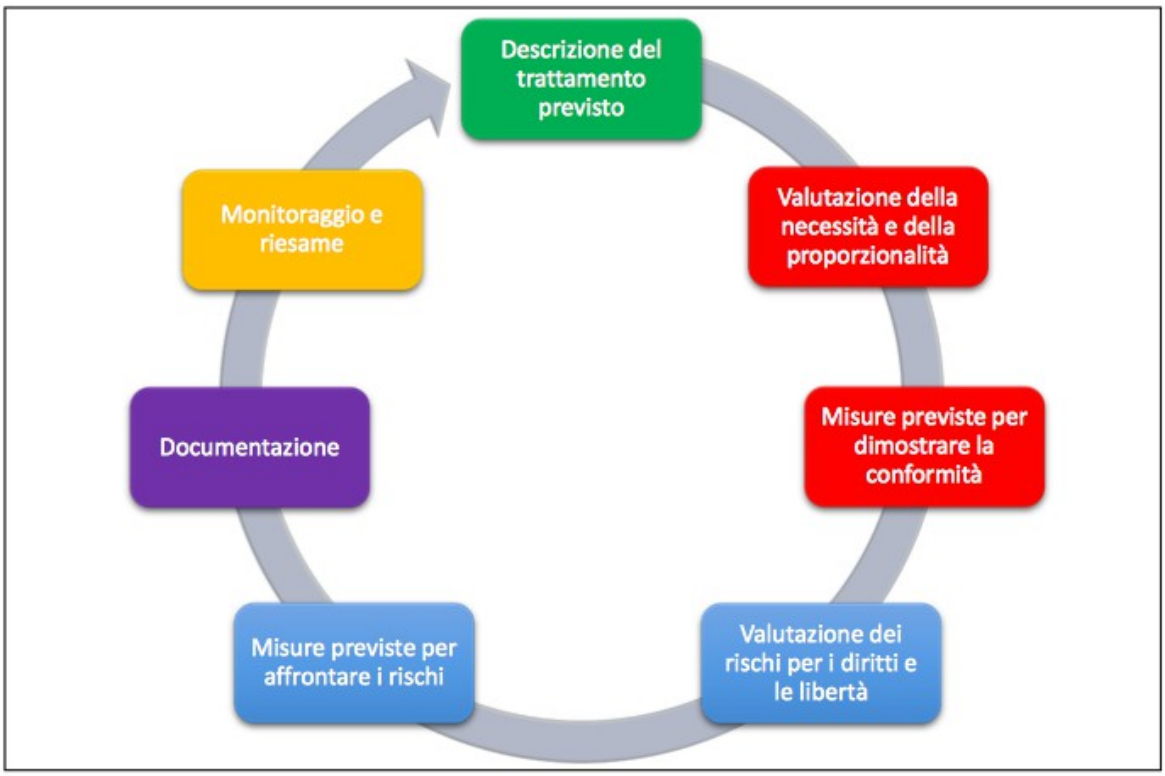
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 09 - Il procedimento inizia con la formazione della lista di leva del Comune stesso e la successiva comunicazione dei soggetti iscritti nelle liste di leva al Distretto militare, quindi vengono costituite le liste di leva ed i registri dei ruoli matricolari. L'Ufficio leva riceve dal distretto militare, le comunicazioni relative agli iscritti di leva dichiarati renitenti, rivedibili e riformati dalle competenti autorita' militari al fine di effettuare le pertinenti annotazioni sulla lista di leva e sui registri dei ruoli matricolari, nonche' per procedere all'adozione di determinazioni ministeriali concernenti i nominativi dei soggetti dichiarati espulsi dall'esercito, cancellati dai ruoli matricolari, ecc.. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000. I dati vengono comunicati al Distretto militare di appartenenza al fine di consentire l'effettuazione delle procedure di arruolamento.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 09 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.P.R. 14.02.1964, n. 237 - L. 31.05.1975, n. 191 - D.Lgs. 18.08.2000, n. 267
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 09 - Sistema informativo relativo all'attivita' relativa alla tenuta delle liste di leva e dei registri matricolari - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 09 - Trattamento effettuato per rilevanti finalita' di interesse pubblico relative a: attivita' relative alla leva militare. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare

copia informatica per consultazione

Rilevanti finalita' di interesse pubblico	- Scheda n. 09 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonche' rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalita' ai sensi dell'art. 2-sexies, comma 2 lett. b) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (leva militare)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 09 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Distretto militare di appartenenza (per le procedure di arruolamento); b) altri comuni e distretti militari (per l'aggiornamento dei ruoli matricolari)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento*	

copia informatica per consultazione

effettuato tramite un sito web- Paese/i di ubicazione del/i server	
Categorie di interessati	- Cittadini italiani
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli

copia informatica per consultazione

interessati o loro rappresentanti	interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Molto alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - livello dell'impatto, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Elettorale: revisione semestrale liste elettorali

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

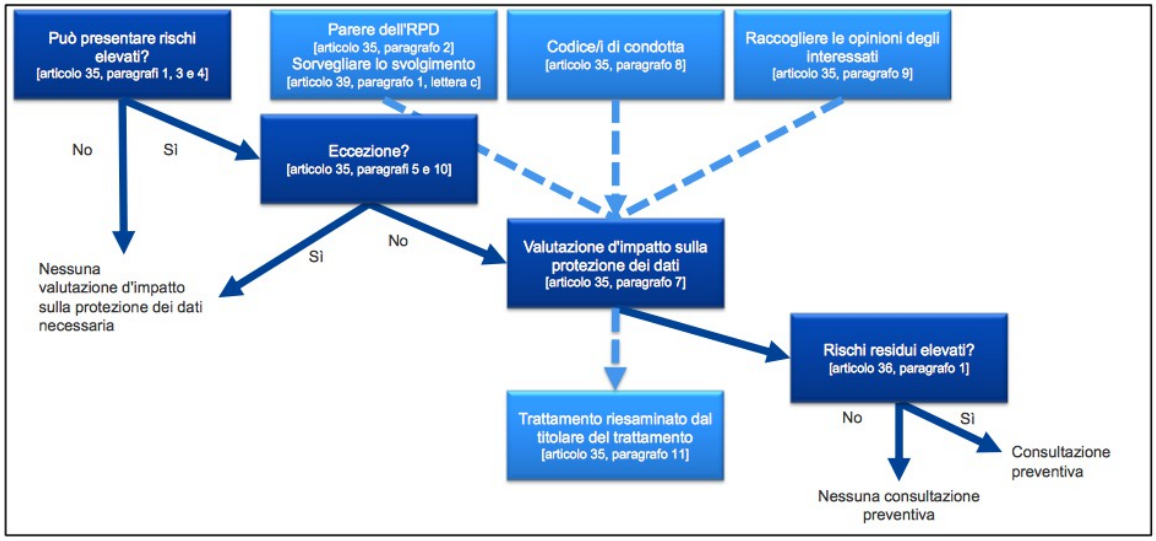
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

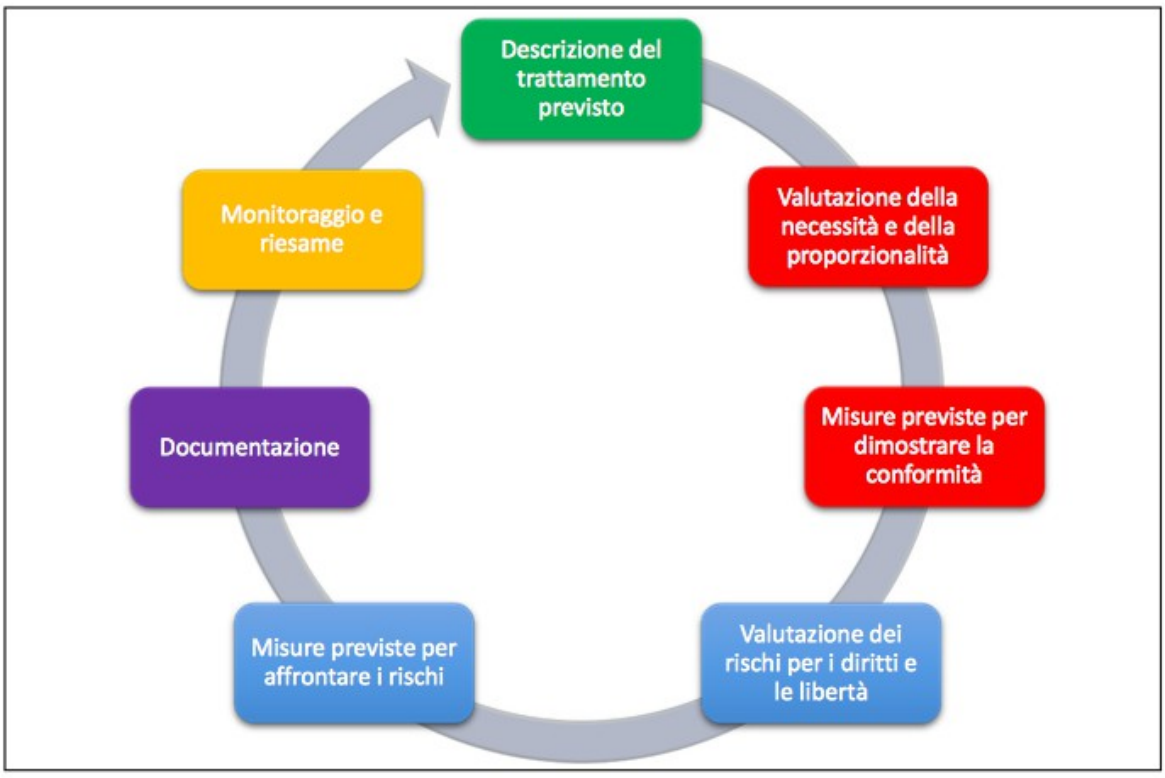
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 27 - I dati giudiziari e sulla salute vengono acquisiti attraverso i controlli svolti sul territorio, che sono effettuati su iniziativa d'ufficio, ovvero su richiesta di privati, di enti e di associazioni; oltre alla verifica in loco, vengono avviati i necessari accertamenti presso gli uffici competenti, al termine dei quali viene predisposta una relazione finale con l'indicazione delle eventuali violazioni in materia sanitaria o ambientale riscontrate. In tal caso, si procede a trasmetterle alle competenti autorita' amministrative o penali. Vengono, inoltre, effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000. Per quanto concerne l'attivita' di polizia mortuaria, ed i connessi servizi cimiteriali, i dati vengono forniti direttamente dagli interessati, dai familiari o dal rappresentante della comunita' religiosa, che presentano apposita domanda al Comune al fine di ottenere delle particolari forme di sepoltura. I dati sulla salute vengono trattati in quanto i medici debbono denunciare al sindaco la malattia che, a loro giudizio, sarebbe stata la causa di morte di persona da loro assistita. Il comune a sua volta comunica le cause di morte all'ISTAT per le rilevazioni annuali, nonche' alla ASL competente per territorio per l'aggiornamento del registro delle cause di morte.

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 27 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 28.02.1985, n. 47 - D.Lgs. 5.02.1997, n. 22 - D.Lgs. 29.10.1999, n. 490 - D.P.R. 10.09.1990, n. 285 - regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 27 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare lo stato di salute: patologie attuali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 27 - Trattamento effettuato per finalita' relative a: attivita' di polizia amministrativa locale, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente compreso l'inquinamento acustico, tutela delle risorse idriche e difesa del suolo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere

copia informatica per consultazione

	ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 27 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di polizia amministrativa locale, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente compreso l'inquinamento acustico, tutela delle risorse idriche e difesa del suolo)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 27 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) ISTAT (per le rilevazioni annuali della cause di morte); b) ASL (per l'aggiornamento del registro delle cause di morte); c) all'ente gestore degli alloggi mortuari (per l'erogazione del servizio)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Persone fisiche - Cittadini italiani - Persone giuridiche ed altri enti (comprende societa' di persone)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Organismi del servizio sanitario nazionale - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati

copia informatica per consultazione

	esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento

copia informatica per consultazione

finalita'	quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza

copia informatica per consultazione

	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli	Alto

copia informatica per consultazione

interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

copia informatica per consultazione

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza:	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica	

copia informatica per consultazione

tecniche logistiche	- MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non

copia informatica per consultazione

	autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante

copia informatica per consultazione

	- MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione e dislocamento delle salme
Gestione delle sepolture e dei loculi

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

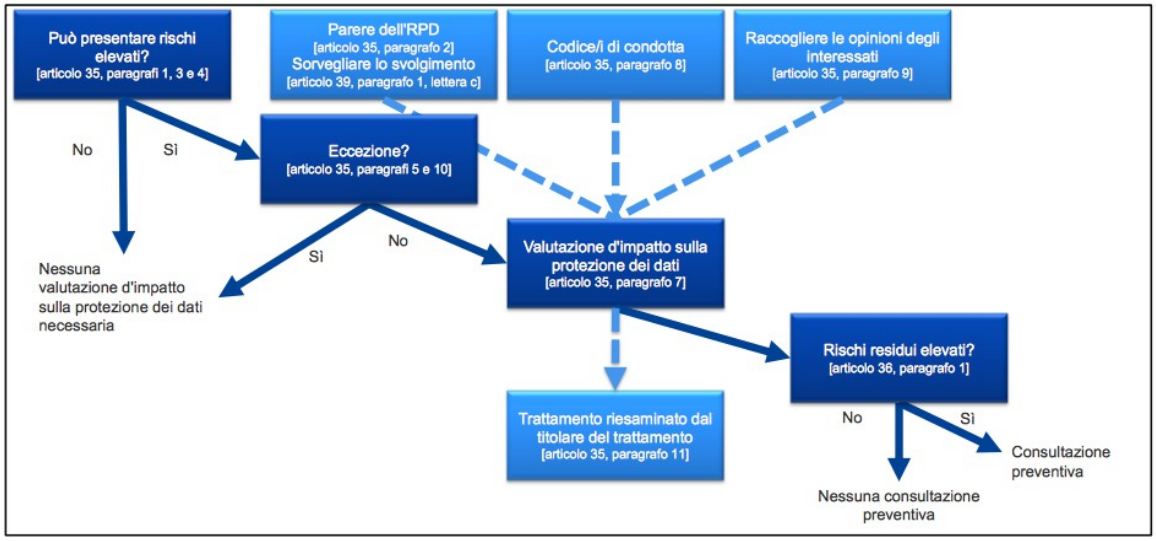
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

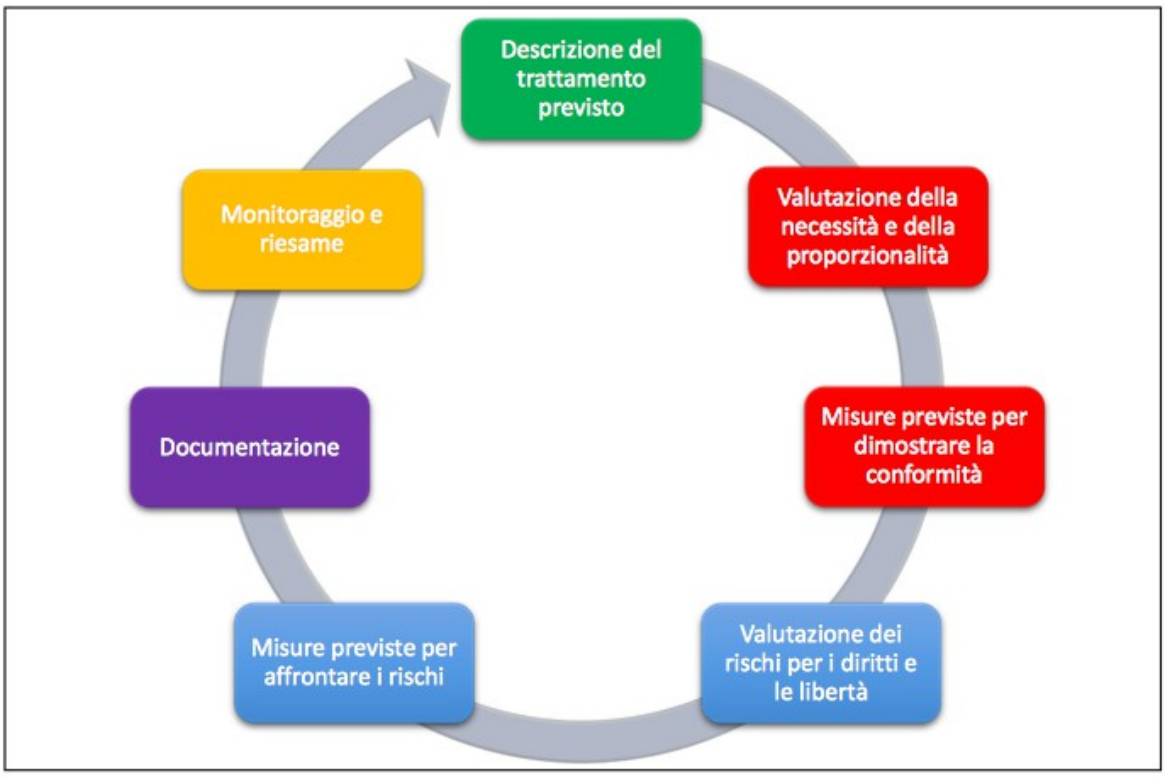
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 42 - I dati vengono acquisiti dagli interessati al momento del sopralluogo e dell'ispezione o verifica; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti o eventuali violazioni rispetto alle dichiarazioni acquisite. I dati sono registrati in archivi/ banche di dati gestite con modalita' elettroniche e su supporti cartacei tramite sistema informativo, controlli esterni, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 42 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - D.Lg. n. 50/2016 - Reg. UE 679/2016 - DL. 24 novembre 1981 n. 689 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sui controlli interni
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 42 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 42 - Trattamento effettuato per attivita' di controllo, ispettive, comprese le attivita' di sopralluogo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 42 -Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di controllo, ispettive, comprese le attivita' di sopralluogo con la polizia locale)
Interesse	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche,

copia informatica per consultazione

legittimo perseguito	nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 42 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Autorita' giudiziaria, autorita' di pubblica sicurezza (per accertamenti di carattere giudiziario); b) al RUP e alla stazione appaltante (D.Lgs. n. 50/2016); c) alle autorita' amministrative di vigilanza (D.Lgs. n. 50/2016)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Persone fisiche - Cittadini italiani

copia informatica per consultazione

	- Persone giuridiche ed altri enti (comprende societa' di persone) - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto

copia informatica per consultazione

Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Accertamento requisiti di dimora abituale delle variazioni di residenza

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

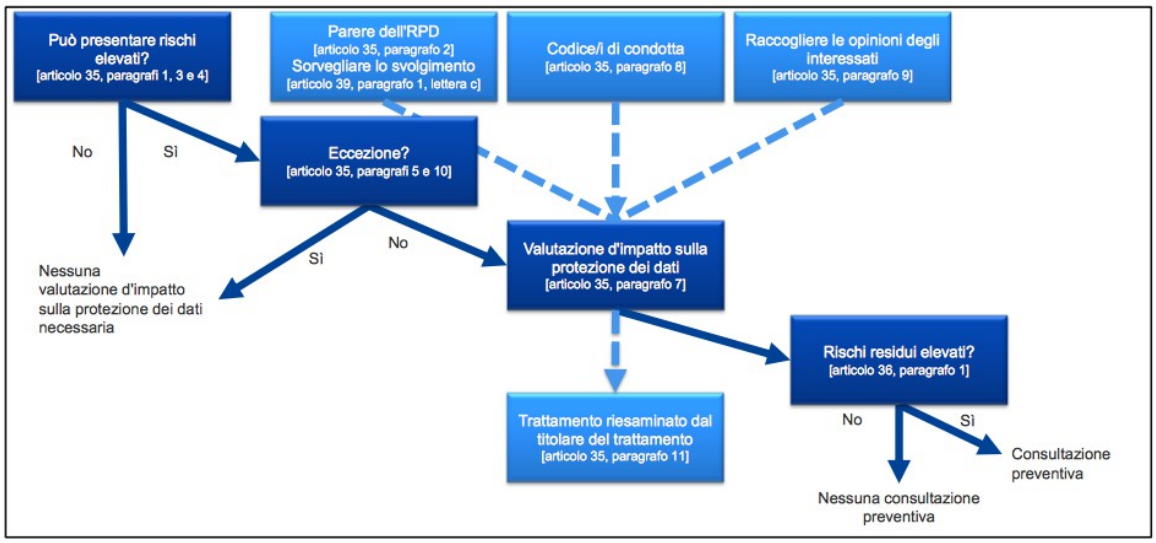
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

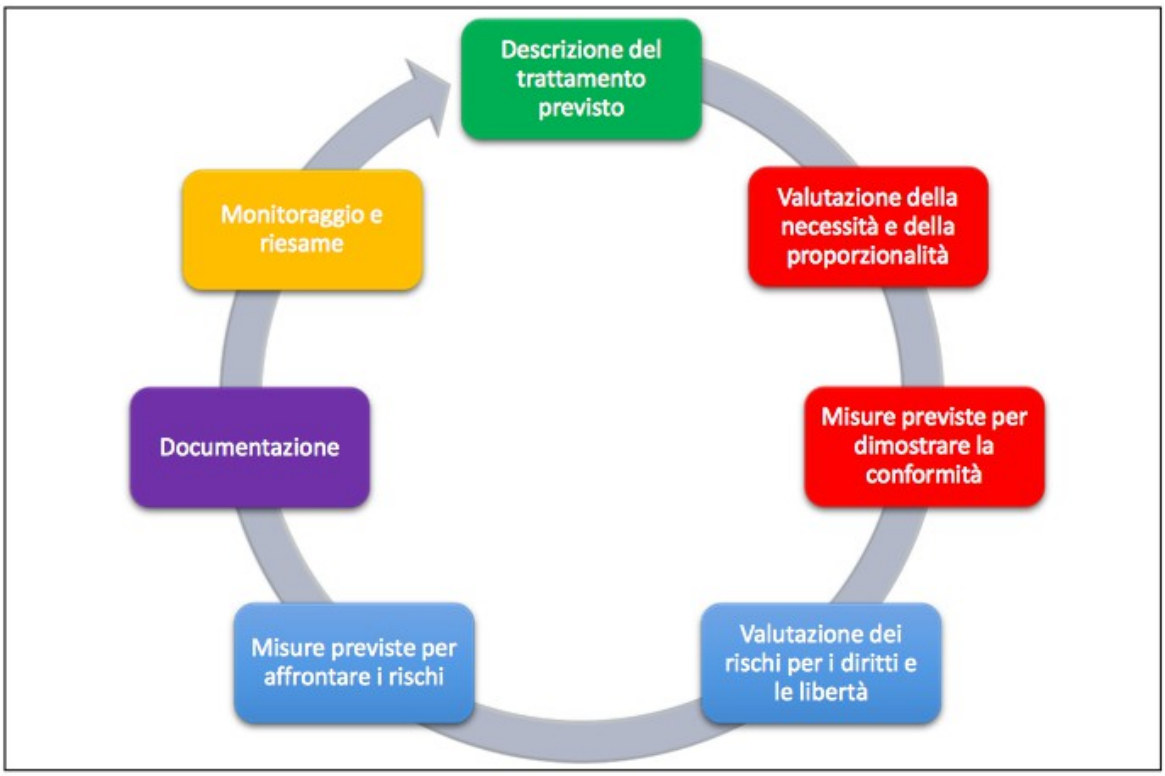
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 41 - Il trattamento di dati personali e' effettuato per la produzione di informazione statistica per il perseguimento delle finalita' istituzionali e in conformita' dell'ambito istituzionale del Comune, fatte salve le specifiche normative di settore. Il trattamento e' effettuato dall'ufficio comunale di statistica. I trattamenti di dati personali sensibili giudiziari debbono essere previsti dal piano annuale delle rilevazioni statistiche o da Rossini dare atto idoneo, adottato sentito il garante, che individui le rilevazioni effettuate dall'ufficio di statistica, anche associato, non facenti parte del programma statistico nazionale, che richiedono il trattamento di dati sensibili, quali tipi di dati sensibili e giudiziari sia necessario trattare, le modalita' di tale trattamento. Il trattamento riguarda indagini statistiche dirette, totali o campionarie; indagini continue in longitudinali; indagini di controllo, di qualita' e di copertura; definizione di disegni campionari e selezione di unita' di rilevazione; costituzione di archivi delle unita' statistiche e di sistemi informativi; elaborazioni statistiche su archivi amministrativi comunali; elaborazione su archivi statistici o amministrativi di altri soggetti pubblici o privati, acquisiti nel rispetto del codice di deontologia e di buona condotta per trattamenti di dati personali a scopi statistici e di ricerca effettuati nell'ambito del sistema statistico nazionale-allegato A D.Lgs. 196/03, e delle direttive del COMSTAT.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 41- Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D. Lgs. n. 322/ 1989-D.Lgs. 267/ 2000- Provvedimento del Garante n. 13 del 31 luglio 2002 - Allegato A D. Lgs. n. 196/.003- Altre fonti ISTAT- Deliberazioni del Comitato di Indirizzo e Coordinamento dell'informazione statistica pubblicate in Gazzetta Ufficiale ISTAT- Circolari pubblicate in Gazzetta Ufficiale- Piano annuale delle rilevazioni statistiche comunali ovvero altro analogo idoneo, adottato sentito il Garante
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 41 - Base di dati: sistema informativo, trattamenti per scopi statistici effettuati da soggetti sistema statistico, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rivelare l'adesione a partiti - Dati idonei a rivelare l'adesione a sindacati - Dati idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale - Dati idonei a rivelare l'origine razziale ed etnica

copia informatica per consultazione

Luoghi di custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 41 - Trattamento effettuato per finalita' di ricerca statistica. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 41 - Trattamenti effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonche' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan) ai sensi dell'art. 2-sexies, comma 2 lett. cc) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (sistema statistico nazionale)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 41 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Soggetti facenti parte del sistema statistico nazionale, nei limiti e con le garanzie di cui al decreto legislativo 322/1989, al codice di deontologia e di buona condotta per il trattamento di dati personali a scopi statistici ricerche effettuati nell'ambito del sistema statistico nazionale
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

dati	
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Codice di deontologia - Trattamento dei dati personali a scopi statistici in ambito Sistan
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Definizione di apposita procedura operativa (PO) per disciplinare le modalita' di collaborazione del responsabile con il titolare ai fini dell'esercizio dei diritti degli interessati - Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza

copia informatica per consultazione

	di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Implicazioni derivanti dalla previsione di cui all'art. 3, comma 1, del d.lgs. n. 33/2013, in base alla quale i dati e i documenti forniti al richiedente tramite l'accesso generalizzato sono considerati come "pubblici" - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento

copia informatica per consultazione

accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare
  3 = alto = = e' **probabile** che la minaccia si possa verificare
  4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

copia informatica per consultazione

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

    - *1 = basso-trascurabile*
    - *2 = medio*
    - *3 = alto*
    - *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e	

copia informatica per consultazione

	relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione

copia informatica per consultazione

sicurezza: procedurali	procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - PROCEDURA OPERATIVA (PO): definire e attuare procedura operativa per dare attuazione, nell'attivita' di videosorveglianza, al principio di c.d. proporzionalita' nella scelta delle modalita' di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonche' nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalita' perseguite - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4

copia informatica per consultazione

Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Statistiche

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria

TRATTAMENTO	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

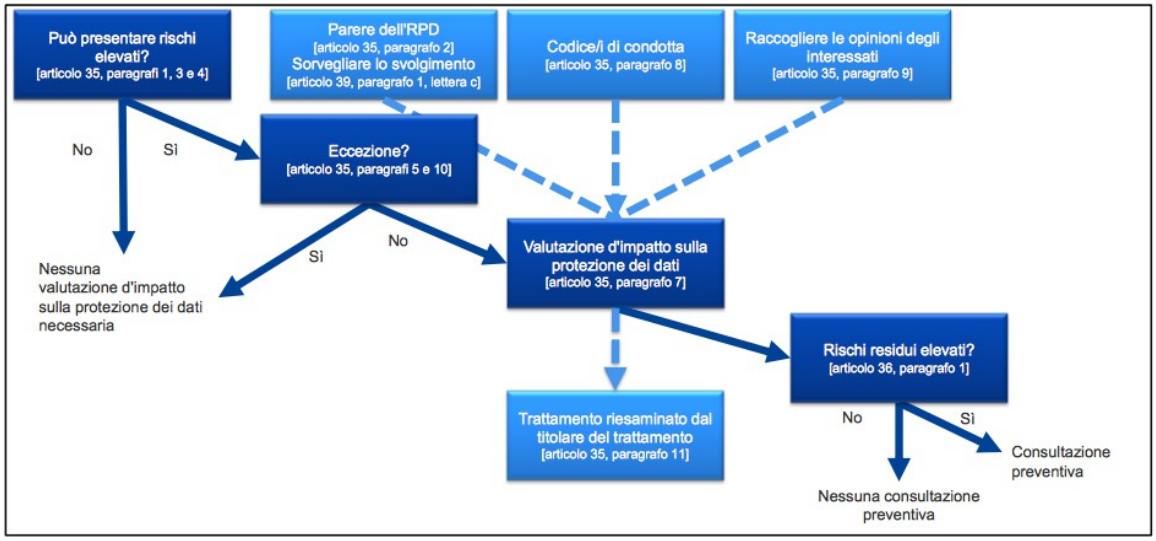
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

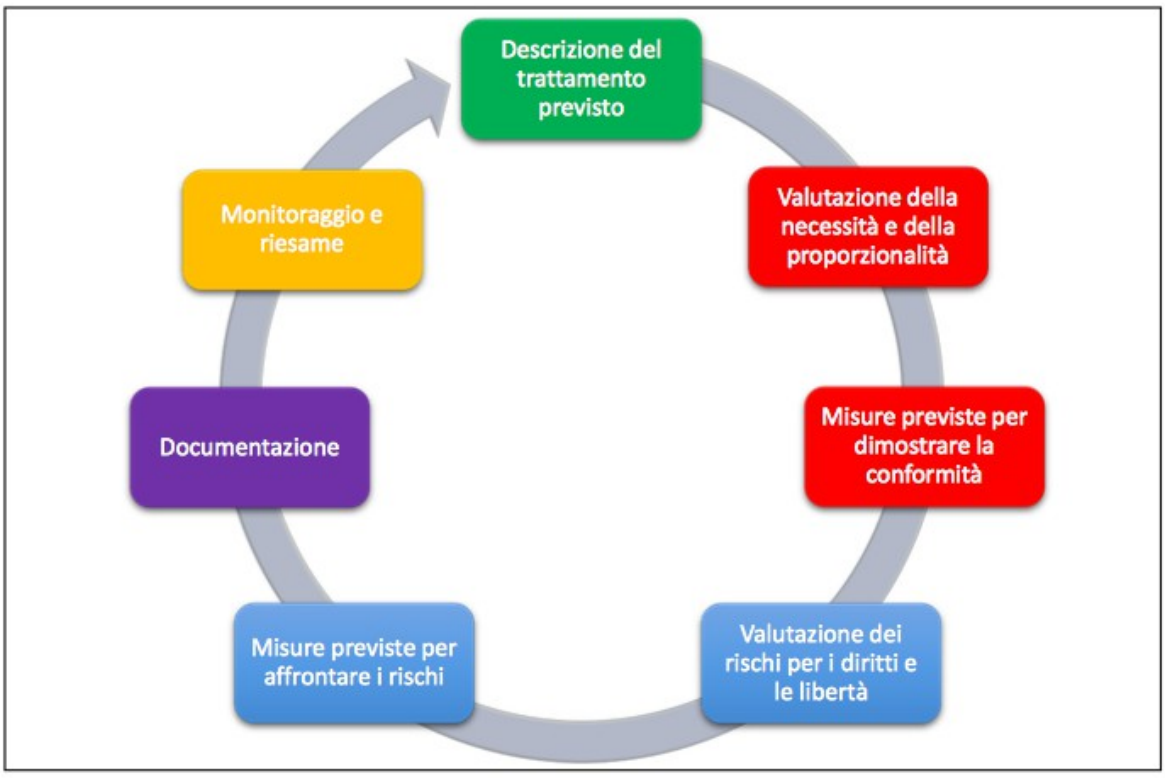
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA
SERVIZIO: denominazione e punti di contatto	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Santinelli Sergio Sig.ra Fiorino Gabriella Sig.ra Giardelli Monica

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 03 - Indipendentemente dall'alto numero di dati contenuti negli archivi anagrafici, quelli di carattere "sensibile" concernono solo le informazioni sull'origine razziale, in quanto tali idonei a rivelare le convinzioni religiose, inseriti negli anni 1938-44 in virtu' delle "leggi razziali"; questi dati, che sono idonei a rivelare in taluni casi anche le convinzioni religiose, non sono comunque resi noti (art. 3, r.d.l. n. 25/1944); le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso. Possono essere altresi' presenti dati sulle patologie pregresse, in considerazione del fatto che fino al 1968 le schede anagrafiche riportavano le cause di decesso

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Fonte normativa	- Scheda n. 03 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (artt. 43 - 47) - L. 24.12.1954, n. 1228 - D.P.R. 30.05.1989, n. 223 - L. 27.10.1988, n. 470 - D.P.R. 06.09.1989, n. 323 - L. 15.5.1997, n. 127 - Legge 27.12.2001, n. 459 - L. 23.10.2003 n. 286 - L. 14.04.1982, n. 164 - D.P.R. 2.04.2003, n. 104
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 03 - Sistema informativo relativo all'anagrafe - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rivelare la vita sessuale (soltanto in caso di eventuale rettificazione di attribuzione di sesso) - Dati idonei a rivelare l'origine razziale (iscrizioni avvenute negli anni 1938-44) - Dati idonei a rilevare le convinzioni religiose (iscrizioni avvenute negli anni 1938-44)
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 03 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: Anagrafe, stato civile e servizio elettorale. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione

copia informatica per consultazione

	europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 03 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonche' rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalita' ai sensi dell'art. 2-sexies, comma 2 lett. b) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (anagrafi della popolazione residente in Italia e di cittadini italiani residenti all'estero)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Cittadini italiani
Categorie di destinatari	- Nessun destinatario per le categorie particolari di dati
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di

copia informatica per consultazione

	valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo

copia informatica per consultazione

	non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Molto alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - livello dell'impatto, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Anagrafe: Comunicazioni Prefettura
Anagrafe: Comunicazioni all'ufficio tributi
Anagrafe: Tenuta registro unioni civili
Anagrafe: Accettazione e tenuta dichiarazioni di testamento biologico
Certificazioni anagrafiche
Anagrafe: Variazioni anagrafiche AIRE (Anagrafe Italiani Residenti all'Estero)
Anagrafe: Iscrizione AIRE (Anagrafe Italiani Residenti all'Estero) dei cittadini italiani per trasferimento da AIRE o APR di altro Comune
Anagrafe: Ripristino immigrazione
Anagrafe: Verifica dichiarazione di rinnovo della dimora abituale
Anagrafe: Attestazione di regolarita' di soggiorno
Anagrafe: Attestazione di soggiorno permanente
Rilascio di documenti di identita'
Anagrafe: Autentica di firma
Anagrafe: Autentica di copia
Anagrafe: Cancellazione anagrafiche AIRE (Anagrafe Italiani Residenti all'Estero)
Anagrafe: Certificati anagrafici storici

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	07 - Attivita' Trasversali
SERVIZIO	Attivita' Trasversali
SERVIZIO	Attivita' Trasversali

TRATTAMENTO	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

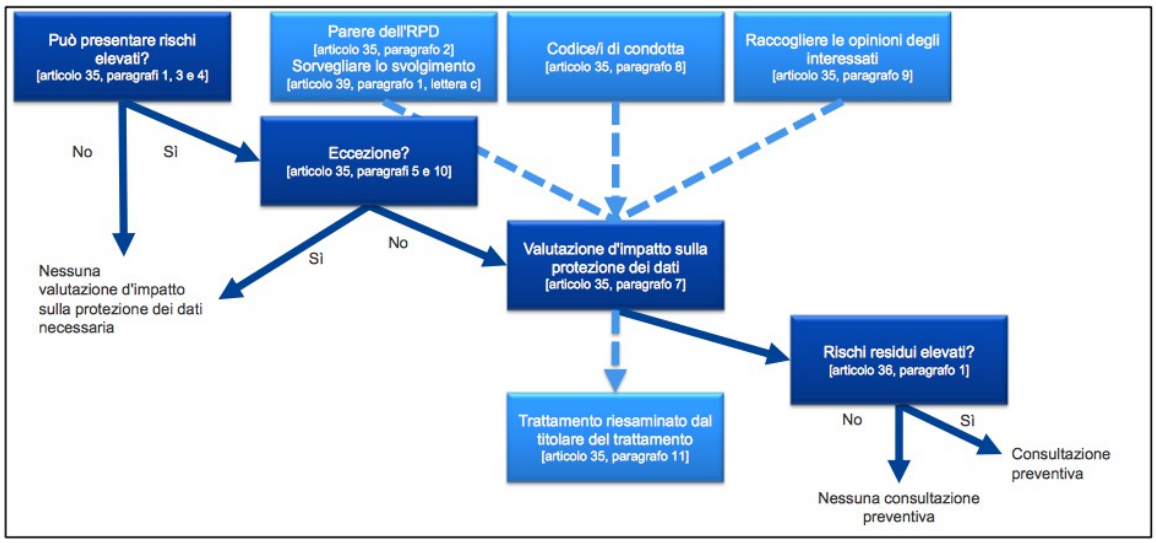
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

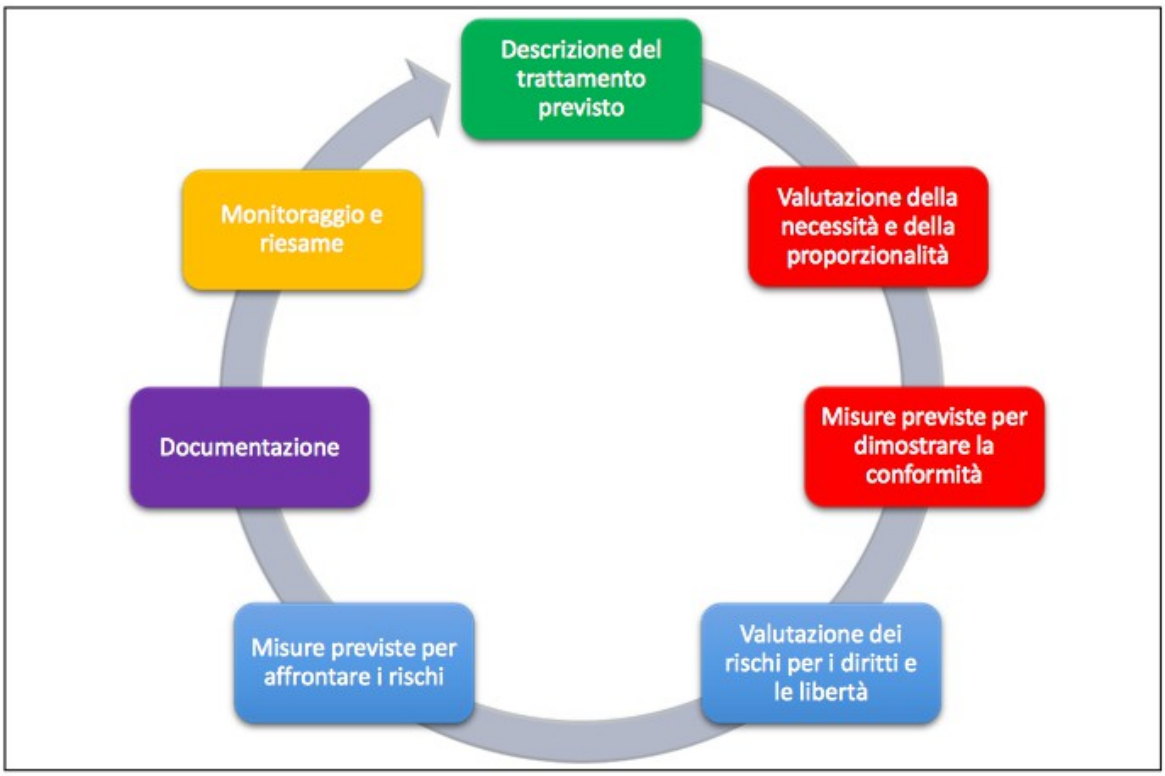
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	07 - Attivita' Trasversali
SERVIZIO	Attivita' Trasversali
SERVIZIO: denominazione e punti di contatto	Attivita' Trasversali
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig.ra Raino' Chiara Sig.ra Rossi Carla

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 33 - Nell'ambito delle proprie prerogative, i consiglieri comunali e gli amministratori possono formulare atti sia di indirizzo politico (quali mozioni, ordini del giorno e risoluzioni), sia di sindacato ispettivo (presentando interrogazioni ed interpellanze alla Giunta comunale), secondo le modalita' stabilite dallo Statuto dal regolamento interno del Consiglio comunale. Le predette attivita' possono comportare il trattamento di dati sensibili e giudiziari riguardanti le persone oggetto di mozioni, ordini del giorno, risoluzioni, interrogazioni o interpellanze. Queste informazioni, eccetto quelle idonee a rivelare lo stato di salute, possono inoltre essere diffuse ai sensi del d.lg. n. 267/200 in ottemperanza al regime di pubblicita' degli atti e delle sedute dei consigli comunali, delle commissioni e degli altri organi comunali (art. 65, comma 5, d.lg. n. 196/2003). Le attivita' ricomprese in questo trattamento sono le attivita' di competenza degli Organi istituzionali (Sindaco, Giunta, Consiglio e commissioni consiliari) nonche' degli Uffici di gestione giuridica del personale dipendente, di Relazioni con il Pubblico.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 33 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 18.08.2000, n. 267 - Statuto e regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza degli Organi istituzionali: Sindaco, Giunta, Consiglio e commissioni consiliari nonche' degli Uffici di gestione giuridica del personale dipendente, di Relazioni con il Pubblico.
Nome archivio/Banca dati	- Scheda n. 33 - Sistema informativo relativo all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare lo stato di salute: anamnesi familiare - Dati idonei a rivelare la vita sessuale
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 33 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: Altri servizi generali. I dati acquisiti vengono trattati esclusivamente per

copia informatica per consultazione

	la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 33 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonche' documentazione delle attivita' istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attivita' di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari ai sensi dell'art. 2-sexies, comma 2 lett. f) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (controllo, di indirizzo politico e di sindacato ispettivo e documentazione dell'attivita' istituzionale di organi pubblici)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 33 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): amministrazioni interessate o partecipi delle questioni oggetto dell'attivita' politica, di controllo e di sindacato ispettivo
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicita' dei lavori dei consigli comunali, delle commissioni e degli altri organi comunali (D.Lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite*	

copia informatica per consultazione

un sito web-nome del dominio del sito web	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Amministratori - Enti locali - Revisori - Segretario comunale
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati

copia informatica per consultazione

	esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento

copia informatica per consultazione

finalita'	quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza

copia informatica per consultazione

	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli	Alto

copia informatica per consultazione

interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

copia informatica per consultazione

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza:	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica	

copia informatica per consultazione

tecniche logistiche	- MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di

copia informatica per consultazione

	impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**

copia informatica per consultazione

art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV DOCUMENTAZIONE (art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV MONITORAGGIO E RIESAME DPIA (art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2

copia informatica per consultazione

	- Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Formazione di determinazioni, ordinanze, decreti ed altri atti amministrativi

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	CONSIGLIO COMUNALE
SERVIZIO	Consiglio comunale e commissioni consiliari

TRATTAMENTO	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

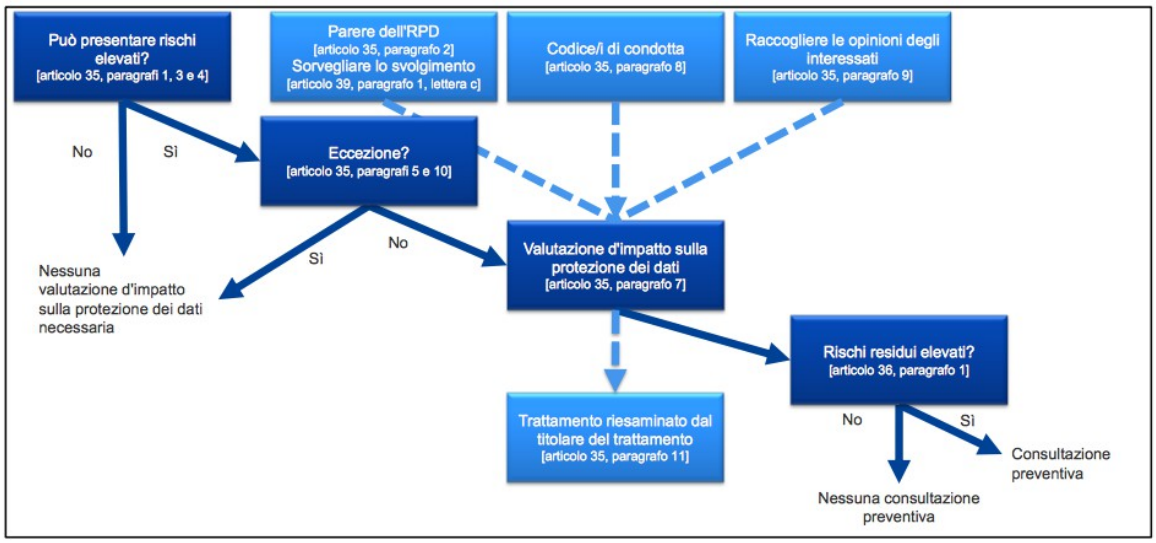
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

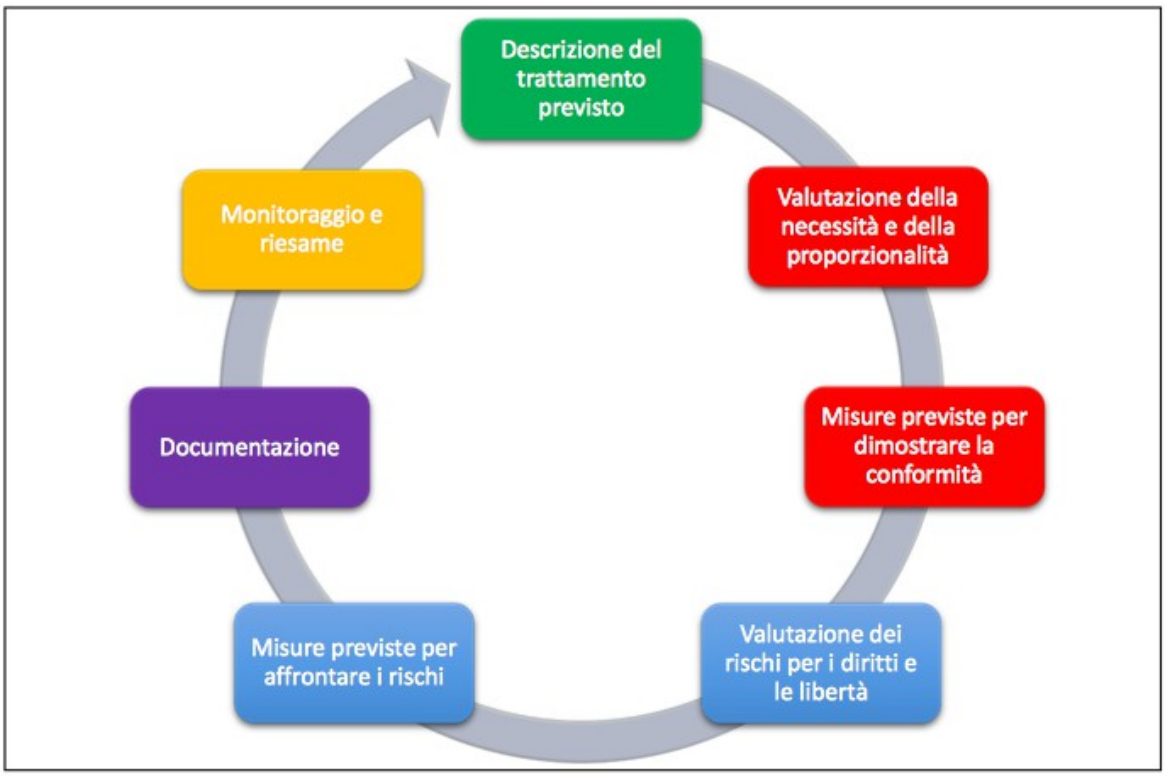
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	CONSIGLIO COMUNALE
SERVIZIO: denominazione e punti di contatto	Consiglio comunale e commissioni consiliari
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 32 - Al fine di valutare eventuali cause ostative alla candidatura dei singoli soggetti, cosi' come per la pronuncia di decadenza di diritto (preventiva o successiva) dall'incarico, vengono acquisiti i dati giudiziari dalla Procura della Repubblica, dall'Ufficio elettorale centrale presso il Tribunale, dalla Prefettura e dal Ministero dell'Interno. Le decisioni in materia di candidabilita', contenenti in particolare la sigla politica di appartenenza dell'interessato, vengono pubblicate all'albo pretorio. Oltre alle informazioni di carattere politico, sindacale, religioso e di altro genere, il comune tratta i dati sanitari degli organi istituzionali al fine di verificare la loro partecipazione alle attivita' dell'ente. I dati vengono diffusi nei casi previsti dalla normativa in vigore (pubblicazione all'albo pretorio delle decisioni in materia di candidabilita' ai sensi d.lgs. n. 267/2000; pubblicita' dell'anagrafe degli amministratori locali ai sensi del citato d.lgs. n. 267/2000). Con riferimento alla nomina del difensore civico, la valutazione del dato politico e giudiziario, in relazione alla presentazione dei curricula, avviene sia a livello politico (da parte dei gruppi consiliari e dei relativi uffici di supporto), sia a livello amministrativo (da parte degli organi del comune, deputati all'istruttoria e alla verifica dei requisiti soggettivi e oggettivi). Il trattamento e' altresi' finalizzato all'accertamento dei requisiti di professionalita' ed onorabilita' dei candidati alle nomine presso enti, aziende e istituzioni. Le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 32 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 18.08.2000, n. 267 (artt. 55 e ss.) - L. 25.03.1993, n. 81 - L. 30.04.1999, n. 120 - L. 5.07.1982, n. 441 - D.P.R. 16.05.1960, n. 570 - L. 19.03.1990, n. 55 (art. 15) - L. 14.04.1982, n. 164
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 32 - Sistema informativo relativo agli organi istituzionali dell'ente - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rilevare convinzioni politiche - Dati comuni identificativi
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 32 - Trattamento effettuato per finalita' relative all'applicazione della disciplina in materia di elettorato attivo e passivo, esercizio del mandato degli organi rappresentativi e di affidamento di incarichi di rappresentanza in enti, aziende e istituzioni nonche' accertamento dei requisiti di onorabilita' e di professionalita' per le nomine a cariche direttive di persone giuridiche. Finalita' ulteriore rispetto a quella per la quale sono raccolti i dati: pagamento emolumenti agli amministratori
Rilevanti finalita' di interesse	- Scheda n. 32 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: esercizio del mandato degli organi rappresentativi,

copia informatica per consultazione

pubblico	ivicompresa la loro sospensione o il loro scioglimento, nonche' l'accertamento delle cause di ineleggibilita', incompatibilita' o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche (art. 2-sexies, comma 2 lett. g) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (applicazione della disciplina in materia di elettorato attivo e passivo, esercizio del mandato degli organi rappresentativi e di affidamento di incarichi di rappresentanza in enti, aziende e istituzioni nonche' accertamento dei requisiti di onorabilita' e di professionalita' per le nomine a cariche direttive di persone giuridiche, e pagamento emolumenti agli amministratori)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 32 - Ministero economia e finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n.164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600) e al Ministero dell'Interno per l'anagrafe degli amministratori locali (ex art. 76 d.lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa):imitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio delle decisioni in materia di candidabilita' (D.Lgs. n. 267/2000) e di anagrafe degli amministratori locali (D.Lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento*	

copia informatica per consultazione

effettuato tramite un sito web- Paese/i di ubicazione del/i server	
Categorie di interessati	- Amministratori
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento:	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa

copia informatica per consultazione

modalita' di cessazione dei dati	comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati

copia informatica per consultazione

	- Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione

copia informatica per consultazione

	professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS** **FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA** **TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS** **FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA** **TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e

copia informatica per consultazione

	formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Istituzione commissioni permanenti, temporanee o speciali

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	CONSIGLIO COMUNALE
SERVIZIO	Consiglio comunale e commissioni consiliari

TRATTAMENTO	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

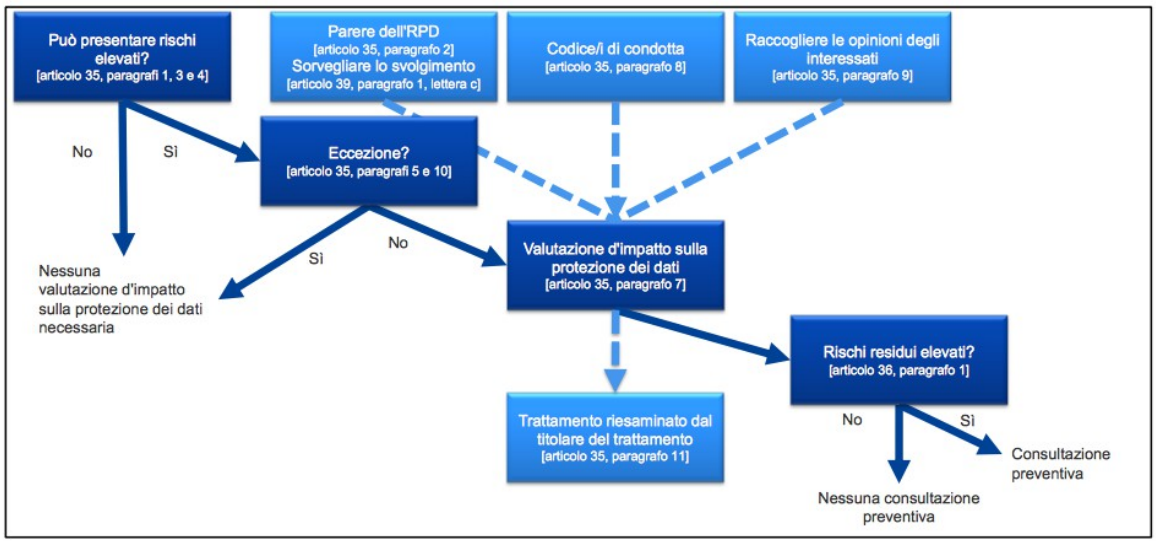
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

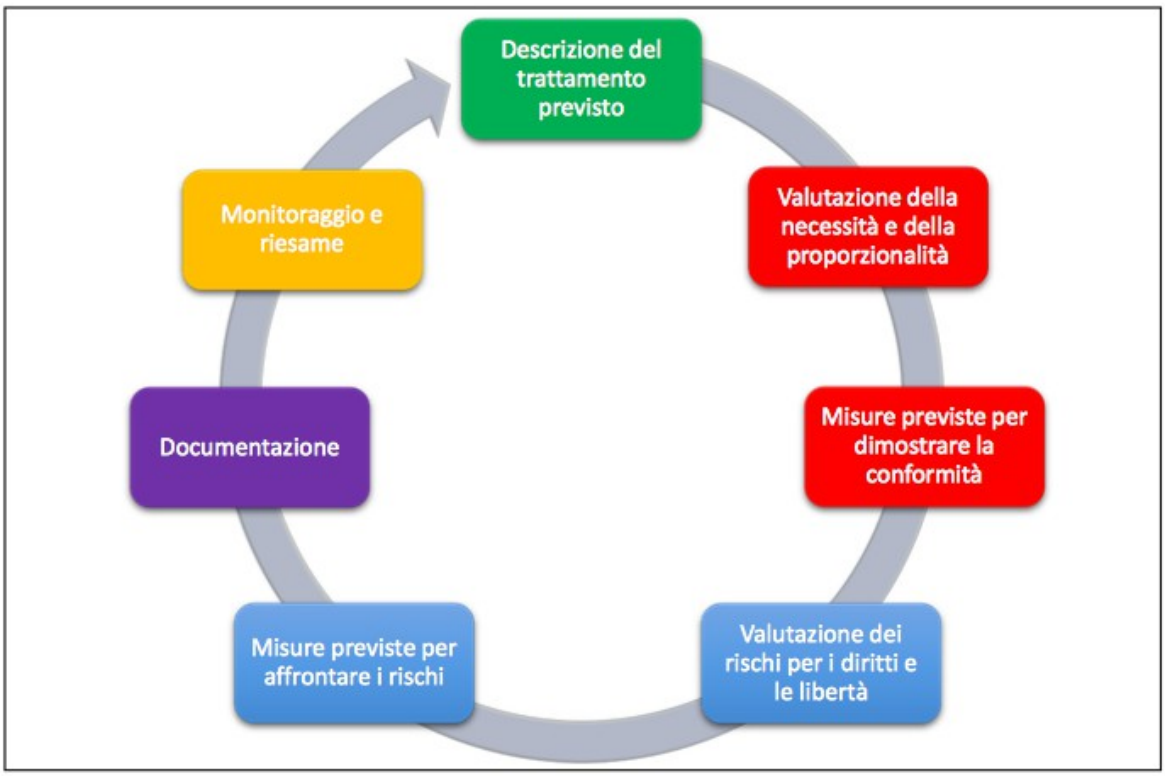
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	CONSIGLIO COMUNALE
SERVIZIO: denominazione e punti di contatto	Consiglio comunale e commissioni consiliari
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 33 - Nell'ambito delle proprie prerogative, i consiglieri comunali e gli amministratori possono formulare atti sia di indirizzo politico (quali mozioni, ordini del giorno e risoluzioni), sia di sindacato ispettivo (presentando interrogazioni ed interpellanze alla Giunta comunale), secondo le modalita' stabilite dallo Statuto dal regolamento interno del Consiglio comunale. Le predette attivita' possono comportare il trattamento di dati sensibili e giudiziari riguardanti le persone oggetto di mozioni, ordini del giorno, risoluzioni, interrogazioni o interpellanze. Queste informazioni, eccetto quelle idonee a rivelare lo stato di salute, possono inoltre essere diffuse ai sensi del d.lg. n. 267/200 in ottemperanza al regime di pubblicita' degli atti e delle sedute dei consigli comunali, delle commissioni e degli altri organi comunali (art. 65, comma 5, d.lg. n. 196/2003). Le attivita' ricomprese in questo trattamento sono le attivita' di competenza degli Organi istituzionali (Sindaco, Giunta, Consiglio e commissioni consiliari) nonche' degli Uffici di gestione giuridica del personale dipendente, di Relazioni con il Pubblico.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 33 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 18.08.2000, n. 267 - Statuto e regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza degli Organi istituzionali: Sindaco, Giunta, Consiglio e commissioni consiliari nonche' degli Uffici di gestione giuridica del personale dipendente, di Relazioni con il Pubblico.
Nome archivio/Banca dati	- Scheda n. 33 - Sistema informativo relativo all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 33 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: Altri servizi generali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita'	- Scheda n. 33 - Trattamento effettuato per rilevanti finalita' di interesse pubblico

copia informatica per consultazione

di interesse pubblico	nella seguente materia: attivita' di elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonche' documentazione delle attivita' istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attivita' di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari ai sensi dell'art. 2-sexies, comma 2 lett. f) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (controllo, di indirizzo politico e di sindacato ispettivo e documentazione dell'attivita' istituzionale di organi pubblici)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 33 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): amministrazioni interessate o partecipi delle questioni oggetto dell'attivita' politica, di controllo e di sindacato ispettivo
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicita' dei lavori dei consigli comunali, delle commissioni e degli altri organi comunali (D.Lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento*	

copia informatica per consultazione

effettuato tramite un sito web- Paese/i di ubicazione del/i server	
Categorie di interessati	- Amministratori - Enti locali - Revisori - Segretario comunale
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai

copia informatica per consultazione

dati	responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che

copia informatica per consultazione

	consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione

copia informatica per consultazione

	professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS** **FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA** **TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS** **FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA** **TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e

copia informatica per consultazione

	formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Mozioni, ordini del giorno, risoluzioni, interrogazioni ed interpellanze

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	CONSIGLIO COMUNALE
SERVIZIO	Consiglio comunale e commissioni consiliari

TRATTAMENTO	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

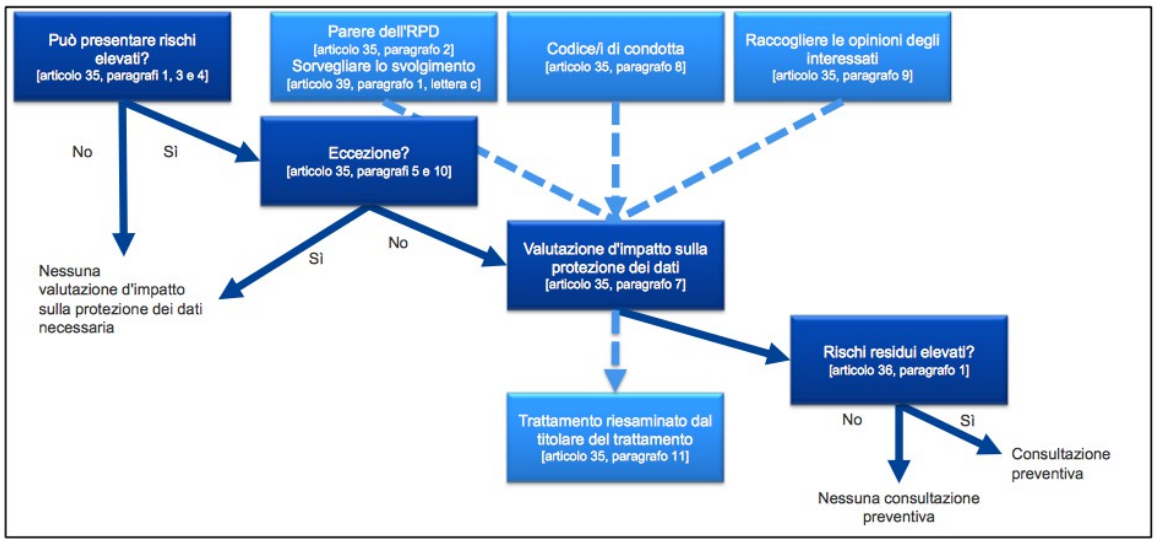
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

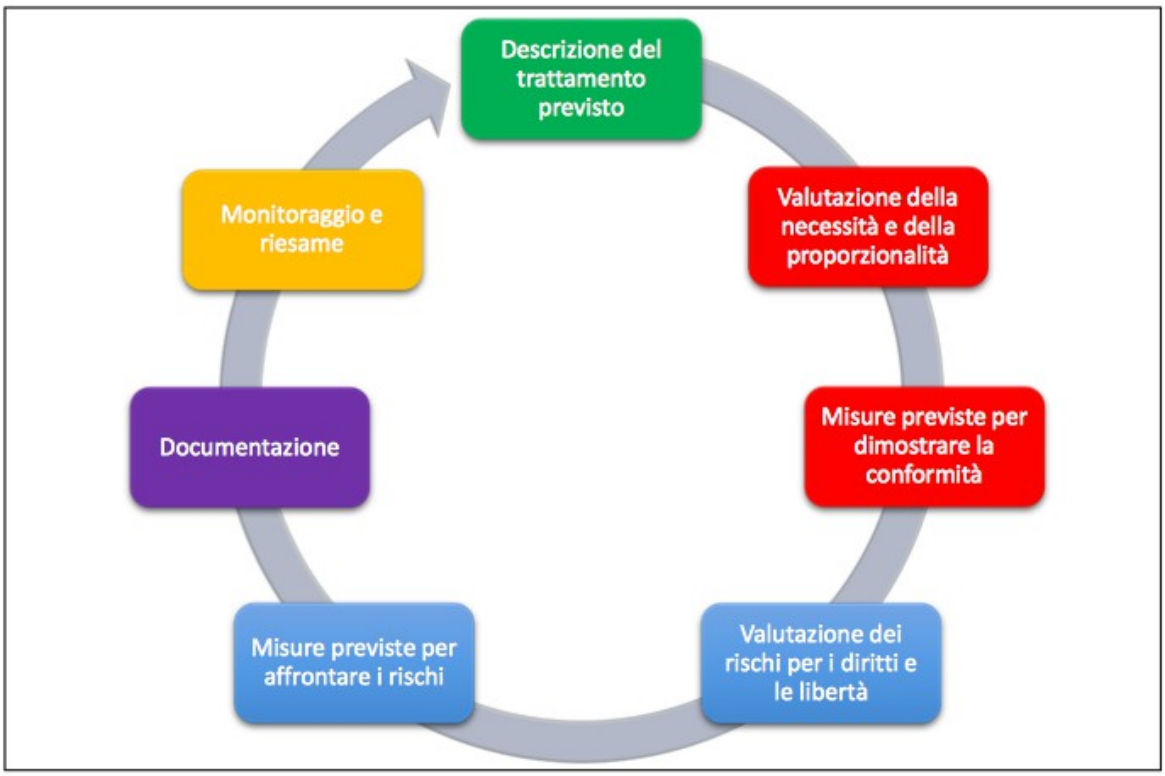
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	CONSIGLIO COMUNALE
SERVIZIO: denominazione e punti di contatto	Consiglio comunale e commissioni consiliari
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 49 - I dati vengono raccolti per la conclusione di transazioni e per la gestione di lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento. Particolari forme di elaborazione tramite interconnessione e raffronto dati con altri soggetti pubblici o privati: amministrazioni certificanti ai sensi del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 49 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento

copia informatica per consultazione

	dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo - Codice Civile - Codice procedura Civile
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 49 - Sistema informativo relativo a beni immobili, demaniali e patrimoniali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare la posizione di beni, strumenti, oggetti
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 49 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 49 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita' di lasciti e transazioni nonche' donazioni e del buon andamento,

copia informatica per consultazione

	dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 49 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) altre amministrazioni e soggetti privati (ai sensi del Regolamento sulla disciplina dei contratti, del Regolamento di contabilita' e della normativa dagli stessi richiamata)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di*	

copia informatica per consultazione

ubicazione del/i server	
Categorie di interessati	- Persone fisiche - Persone giuridiche ed altri enti (comprende societa' di persone)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III

copia informatica per consultazione

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete

copia informatica per consultazione

	internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli	Alto

copia informatica per consultazione

interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

copia informatica per consultazione

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza:	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da	

copia informatica per consultazione

tecniche informatiche, comprese le misure di ripristino in caso di data breach	consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di

copia informatica per consultazione

	ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Lasciti e donazioni

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Gestione Patrimonio Immobiliare
SERVIZIO	Gestione Patrimonio Immobiliare

TRATTAMENTO	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

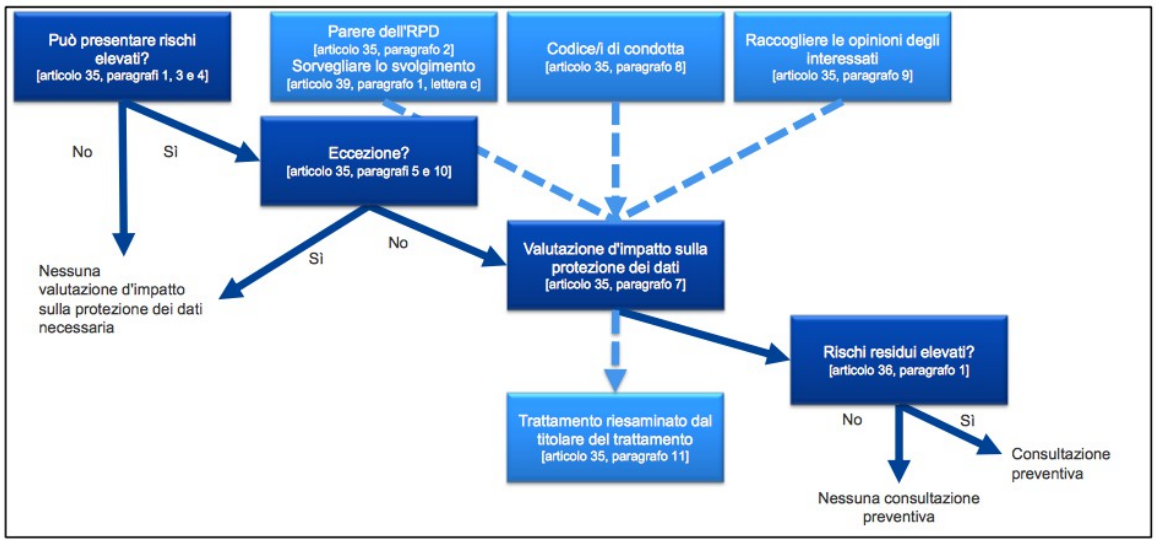
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

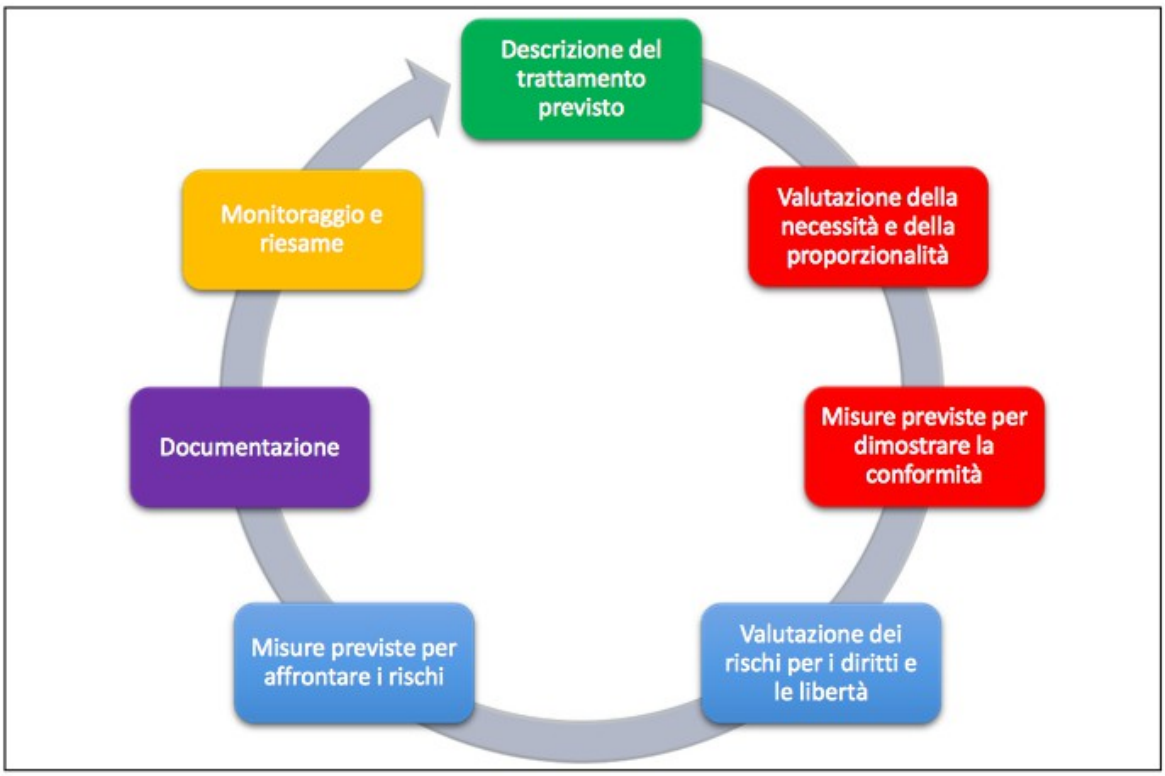
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Gestione Patrimonio Immobiliare
SERVIZIO: denominazione e punti di contatto	Gestione Patrimonio Immobiliare
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Arch. Braccesi Priscilla
Incaricati trattamento: denominazione e punti di contatto	sig. Cavicchioli Gaetano Dott.ssa Mazzanti Agnese sig. Corsi Francesco Dott. Dini Carlo Sig. Pisani Yuri

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 20 - Con riferimento alle attivita' relative alla concessione di benefici, all'assegnazione degli alloggi di edilizia residenziale pubblica (che comprende anche l'attivita' di valutazione dei requisiti ai fini dell'eventuale riduzione dei canoni di locazione degli alloggi di proprieta' comunale), nonche' alle esenzioni di carattere tributario, il trattamento di dati sensibili si rende necessario sia per la concessione o l'assegnazione stesse, sia per la predisposizione delle graduatorie dei beneficiari. Le informazioni relative alla terapia in corso vengono trattate durante la fase istruttoria riguardante l'erogazione di contributi per sostenere l'acquisto di farmaci. I dati vengono forniti direttamente dagli interessati, che presentano apposita domanda al Comune, oppure da terzi (anagrafe, autorita' giudiziaria, ASL, provincia, altri servizi comunali, i quali effettuano dei servizi di sostegno in favore dell'utente che versa in stato di indigenza). I dati vengono comunicati, in particolare, all'ente gestore degli alloggi che procede alla relativa assegnazione. Vengono, inoltre, effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.
Con riferimento alle attivita' relative alla concessione di benefici, sia in campo sociale che nel campo dello sviluppo economico, il trattamento dei dati si rende necessario sia per la concessione o l'assegnazione degli stessi, sia per la predisposizione delle graduatorie, che vengono rese pubbliche ove previsto dalla relativa normativa, fermo

copia informatica per consultazione

restando il divieto di diffondere i dati sulla salute ai sensi degli artt. 22, comma 8, e 68, comma 3, del d.lg. n. 196/2003.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 20 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 15.02.1980, n. 25 - D.Lgs. 30.12.1992, n. 504 - D.Lgs. 25.07.1998, n. 286 (art. 40) - L. 9.12.1998, n. 431 (art. 11, c. 8) - D.Lgs. 30.12.1992, n. 504 - D.Lgs. 15.11.1993, n. 507 - Leggi regionali - regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 20 - Sistema informativo relativo alle attivita' relative alla concessione di benefici economici e agli interventi di sostegno per la problematica abitativa, comprese le assegnazioni/conservazioni di alloggi di edilizia residenziale pubblica - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di	- In Italia

copia informatica per consultazione

custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 20 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: attivita' dirette all'applicazione, anche tramite concessionari, delle disposizioni in materia di tributi; concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti ed abilitazioni; assegnazione di alloggi di edilizia residenziale pubblica. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 20 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nelle seguenti materie: - attivita' dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale ai sensi dell'art. 2-sexies, comma 2, lett. i), D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018; - concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti ed abilitazioni ai sensi dell'art. 2-sexies, comma 2, lett. m), D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018; - assegnazione di alloggi di edilizia residenziale pubblica ai sensi dell'art. 2-sexies, comma 2, lett. m), D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 20 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Ente gestore degli alloggi (per la relativa assegnazione)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trasferimento all'estero***	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Utenti (anche potenziali)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati	

copia informatica per consultazione

personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi

copia informatica per consultazione

	preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori

copia informatica per consultazione

indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e

copia informatica per consultazione

	utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento

copia informatica per consultazione

accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare
  3 = alto = = e' **probabile** che la minaccia si possa verificare
  4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

copia informatica per consultazione

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

    - *1 = basso-trascurabile*
    - *2 = medio*
    - *3 = alto*
    - *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e	

copia informatica per consultazione

	aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai

copia informatica per consultazione

	sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	FRAMEWORKS FUNZIONE
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai

copia informatica per consultazione

	registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS** **FUNZIONE**
art. 35	**Monitorare**
CRITERI **LINEE GUIDA**	**DPIA** **TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

copia informatica per consultazione

Assegnazione Alloggi Edilizia Residenziale Pubblica - E.R.P.

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Gestione Patrimonio Immobiliare
SERVIZIO	Gestione Patrimonio Immobiliare

TRATTAMENTO	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

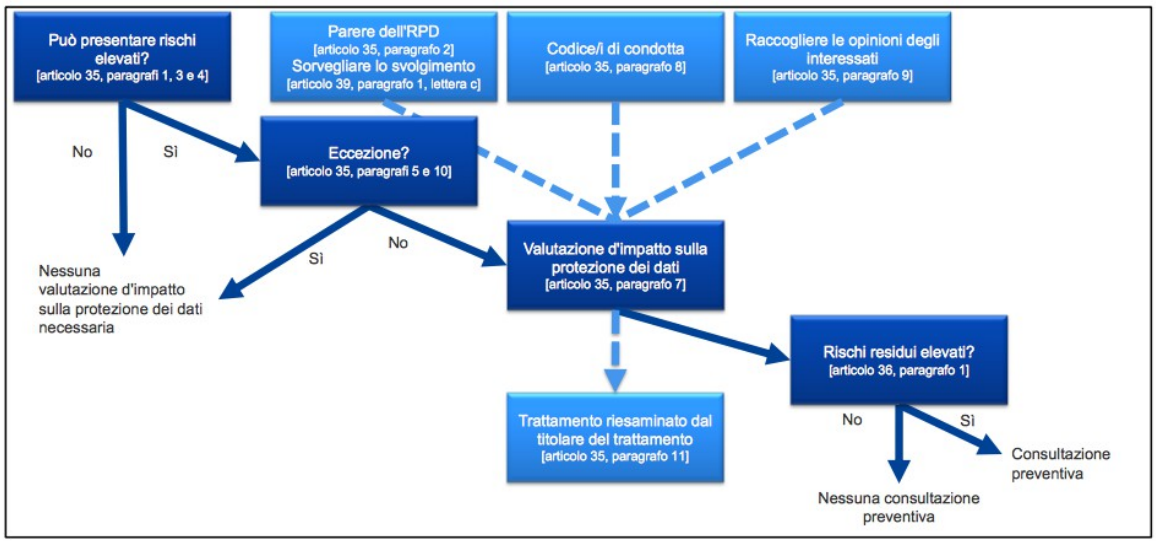
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

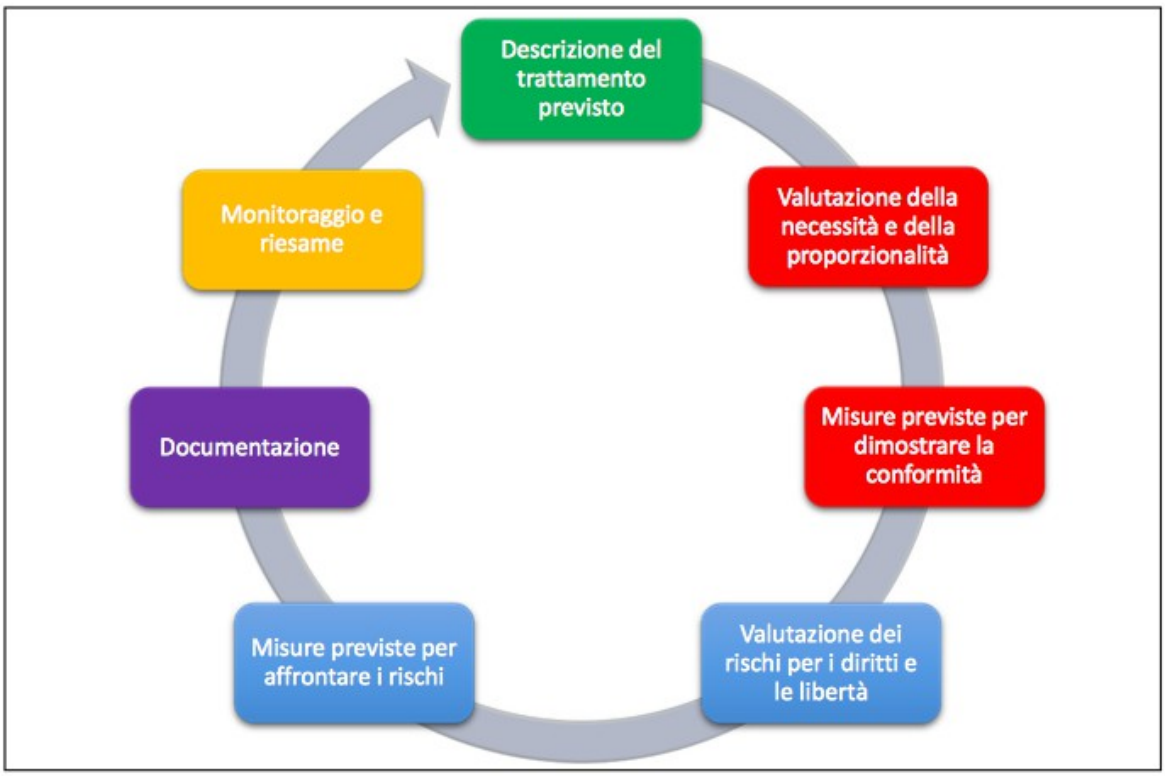
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Gestione Patrimonio Immobiliare
SERVIZIO: denominazione e punti di contatto	Gestione Patrimonio Immobiliare
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Arch. Braccesi Priscilla
Incaricati trattamento: denominazione e punti di contatto	sig. Cavicchioli Gaetano Dott.ssa Mazzanti Agnese sig. Corsi Francesco Dott. Dini Carlo Sig. Pisani Yuri

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 27 - I dati giudiziari e sulla salute vengono acquisiti attraverso i controlli svolti sul territorio, che sono effettuati su iniziativa d'ufficio, ovvero su richiesta di privati, di enti e di associazioni; oltre alla verifica in loco, vengono avviati i necessari accertamenti presso gli uffici competenti, al termine dei quali viene predisposta una relazione finale con l'indicazione delle eventuali violazioni in materia sanitaria o ambientale riscontrate. In tal caso, si procede a trasmetterle alle competenti autorita' amministrative o penali. Vengono, inoltre, effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000. Per quanto concerne l'attivita' di polizia mortuaria, ed i connessi servizi cimiteriali, i dati vengono forniti direttamente dagli interessati, dai familiari o dal rappresentante della comunita' religiosa, che presentano apposita domanda al Comune al fine di ottenere delle particolari forme di sepoltura. I dati sulla salute vengono trattati in quanto i medici debbono denunciare al sindaco la malattia che, a loro giudizio, sarebbe stata la causa di morte di persona da loro assistita. Il comune a sua volta comunica le cause di morte all'ISTAT per le rilevazioni annuali, nonche' alla ASL competente per territorio per l'aggiornamento del registro delle cause di morte.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 27 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 28.02.1985, n. 47 - D.Lgs. 5.02.1997, n. 22 - D.Lgs. 29.10.1999, n. 490 - D.P.R. 10.09.1990, n. 285 - regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 27 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare lo stato di salute: patologie attuali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 27 - Trattamento effettuato per finalita' relative a: attivita' di polizia amministrativa locale, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente compreso l'inquinamento acustico, tutela delle risorse idriche e difesa del suolo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare

copia informatica per consultazione

Rilevanti finalita' di interesse pubblico	- Scheda n. 27 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di polizia amministrativa locale, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente compreso l'inquinamento acustico, tutela delle risorse idriche e difesa del suolo)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 27 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) ISTAT (per le rilevazioni annuali della cause di morte); b) ASL (per l'aggiornamento del registro delle cause di morte); c) all'ente gestore degli alloggi mortuari (per l'erogazione del servizio)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Persone fisiche - Cittadini italiani - Persone giuridiche ed altri enti (comprende societa' di persone)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Organismi del servizio sanitario nazionale - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati

copia informatica per consultazione

	esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento

copia informatica per consultazione

finalita'	quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza

copia informatica per consultazione

	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli	Alto

copia informatica per consultazione

interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

copia informatica per consultazione

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza:	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica	

copia informatica per consultazione

tecniche logistiche	- MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti

copia informatica per consultazione

	- MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

copia informatica per consultazione

l'applicazione delle misure	

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Accertamento requisiti di dimora abituale delle variazioni di residenza

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Gestione Patrimonio Immobiliare
SERVIZIO	Gestione Patrimonio Immobiliare

TRATTAMENTO	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

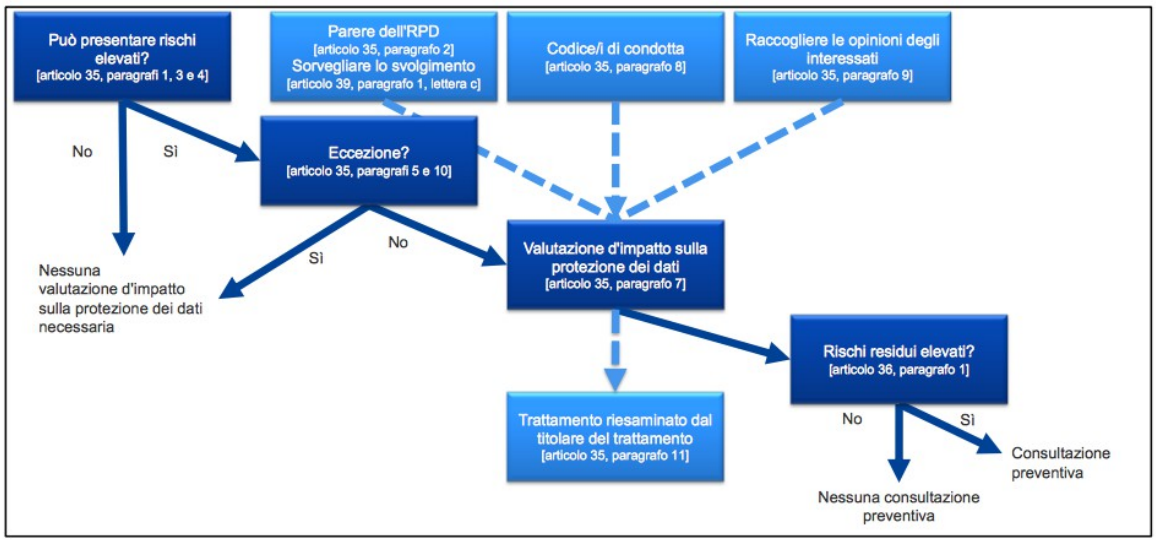
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

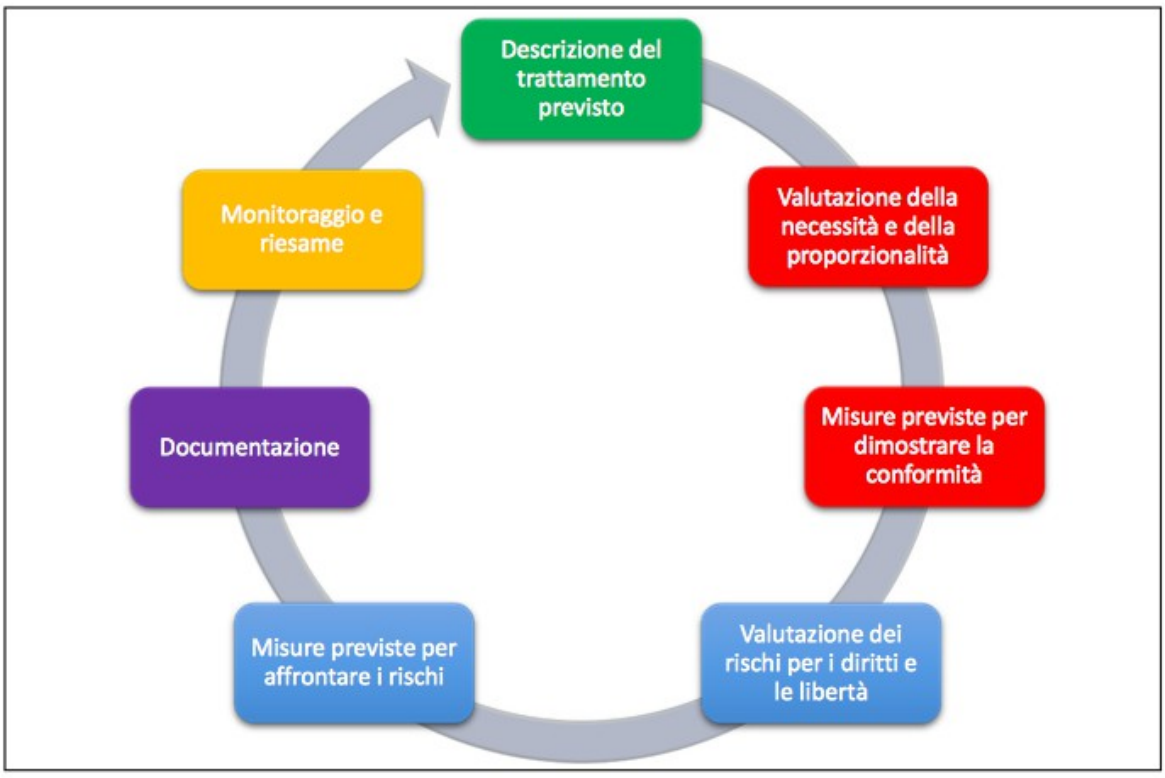
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Gestione Patrimonio Immobiliare
SERVIZIO: denominazione e punti di contatto	Gestione Patrimonio Immobiliare
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Arch. Braccesi Priscilla
Incaricati trattamento: denominazione e punti di contatto	sig. Cavicchioli Gaetano Dott.ssa Mazzanti Agnese sig. Corsi Francesco Dott. Dini Carlo Sig. Pisani Yuri

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 50 - Il trattamento ha per oggetto i dati delle procedure di affidamento e dei contratti di appalto e di concessione delle amministrazioni aggiudicatrici e degli enti aggiudicatori per l'acquisizione di servizi, forniture, lavori e opere, nonche' i concorsi pubblici di progettazione e l'attivita' posta in essere in attuazione del D.Lgs. n. 50/2016. I dati vengono raccolti dai soggetti partecipanti alle procedure di affidamento e includono dati sensibili e giudiziari. Il trattamento implica, oltre alle ordinarie forme di elaborazione standardizzate (con mezzi elettronici e su supporto cartaceo), anche la comunicazione a terzi e, in particolare, alle Autorita' competenti a rilasciare le certificazioni sul possesso dei requisiti, nonche' la possibile diffusione mediante pubblicazione sul profilo del committente e sui siti web prescritti dalla normativa vigente in materia.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo - D.Lgs. 267/2000 T.U.E.L. - D.Lgs. 50/2016
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza trasversalmente, di tutti gli uffici che aggiudicano contratti inclusi nell'ambito di applicazione del D.Lgs. 50 n. 0/2016
Nome archivio/Banca dati	- Scheda n. 50 - Sistema informativo relativo ad appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati comuni, diversi dai dati particolari - Dati di accesso e di identificazione (user name, password, customer ID, altro) - Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili - Dati relativi al comportamento debitorio - Dati relativi all'affidabilita' o puntualita' nei pagamenti - Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati relativi all'adempimento di obbligazioni - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a

copia informatica per consultazione

	comportamenti illeciti o fraudolenti - Dati sensibili - Dati relativi all'affidabilita' nell'esecuzione dei contratti pubblici - Dati comuni identificativi - Indirizzo di posta elettronica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 50 - Trattamento effettuato per finalita' di adempimento di obblighi contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 50 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Altre amministrazioni ed enti pubblici - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi - Scheda n. 50 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Agenzia Entrate, Prefettura, Tribunale, Procura presso il Tribunale, Provincia e altri enti pubblici - INPS/INAIL/ANAC - , anche

copia informatica per consultazione

	attraverso la consultazione delle relative Banche dati, per i controlli sul possesso dei requisiti dichiarati in sede di procedura di affidamento; b) altri soggetti partecipanti alla procedura di affidamento; c) consulenti e soggetti, pubblici o privati, che effettuano servizi di committenza ausiliaria; d) avvocati incaricati dell'eventuale contenzioso (ai sensi del D.Lgs. n. 50/2016 e della regolazione attuativa)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione sul sito web, in "Amministratrazione trasparente" in attuazione di obblighi di pubblicazione di cui al D. Lgs. n. 33/2013 - Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Utenti (anche potenziali) - Concorrenti alle procedure di affidamento di contratti pubblici - Soggetti terzi rispetto ai concorrenti, i cui dati rilevano nella procedura di affidamento
Categorie di destinatari	- Amministrazioni dello Stato - Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3

copia informatica per consultazione

	della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione

copia informatica per consultazione

	del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle

copia informatica per consultazione

	specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI **Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati** (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA INCIDENTI: crimeware (malware che mirano a ottenere il controllo dei sistemi) - CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento -TRATTAMENTI ELETTRONICI: utilizzo di parole chiave non adeguate - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	
STIMA (XxY)	

copia informatica per consultazione

DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e	

copia informatica per consultazione

	implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di

copia informatica per consultazione

	consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al regolamento generale sulla protezione dei dati e' provata dal documento di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dal documento di DPIA - La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessione a titolo gratuito delle sale e immobili del patrimonio comunale
Concessioni canali demaniali irrigui
Locazione immobili urbani
Vendita beni patrimonio disponibile mediante asta pubblica

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	GIUNTA COMUNALE
SERVIZIO	Giunta comunale

TRATTAMENTO	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

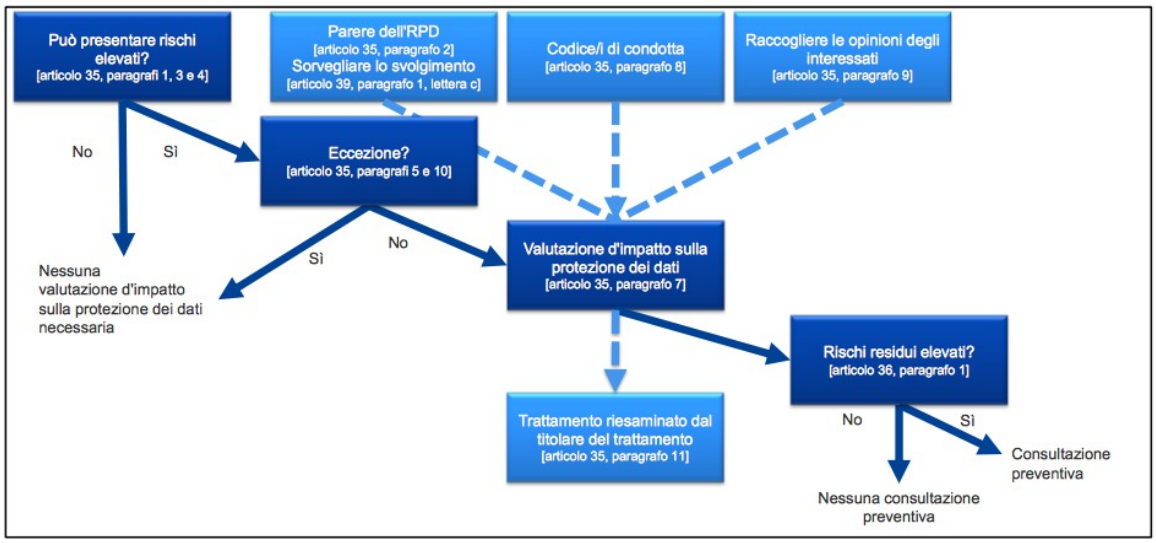
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

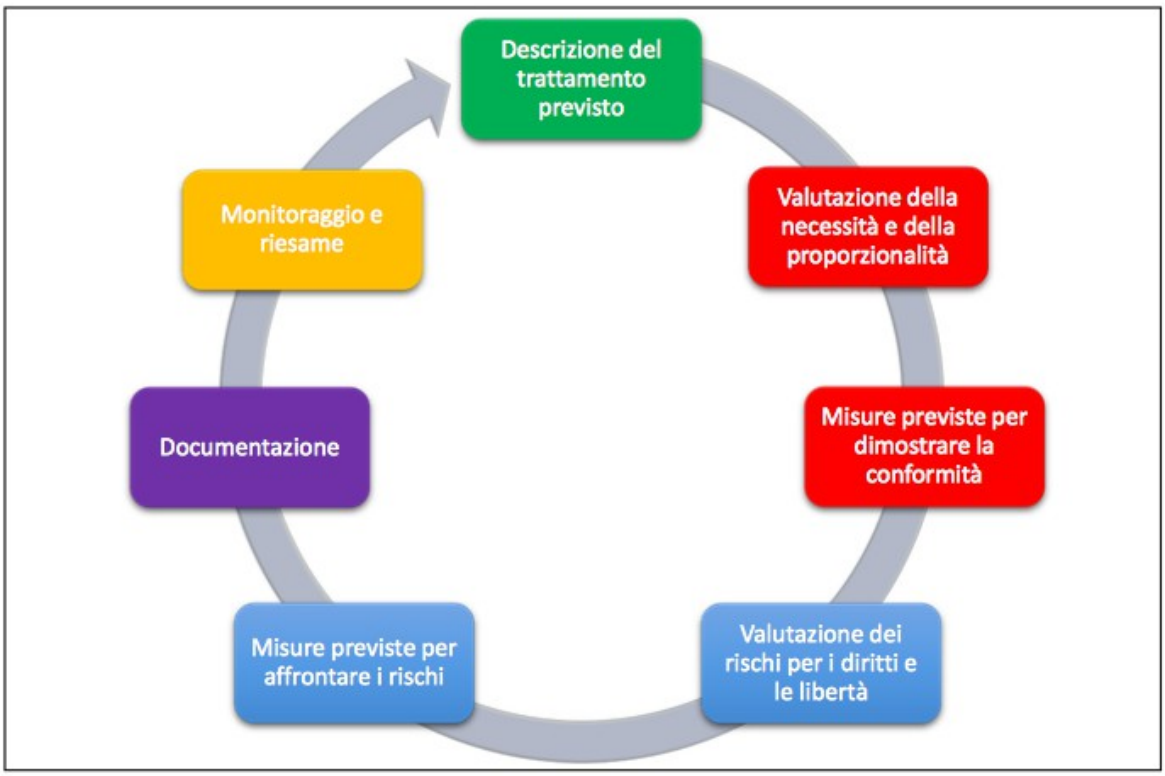
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	GIUNTA COMUNALE
SERVIZIO: denominazione e punti di contatto	Giunta comunale
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 32 - Al fine di valutare eventuali cause ostative alla candidatura dei singoli soggetti, cosi' come per la pronuncia di decadenza di diritto (preventiva o successiva) dall'incarico, vengono acquisiti i dati giudiziari dalla Procura della Repubblica, dall'Ufficio elettorale centrale presso il Tribunale, dalla Prefettura e dal Ministero dell'Interno. Le decisioni in materia di candidabilita', contenenti in particolare la sigla politica di appartenenza dell'interessato, vengono pubblicate all'albo pretorio. Oltre alle informazioni di carattere politico, sindacale, religioso e di altro genere, il comune tratta i dati sanitari degli organi istituzionali al fine di verificare la loro partecipazione alle attivita' dell'ente. I dati vengono diffusi nei casi previsti dalla normativa in vigore (pubblicazione all'albo pretorio delle decisioni in materia di candidabilita' ai sensi d.lgs. n. 267/2000; pubblicita' dell'anagrafe degli amministratori locali ai sensi del citato d.lgs. n. 267/2000). Con riferimento alla nomina del difensore civico, la valutazione del dato politico e giudiziario, in relazione alla presentazione dei curricula, avviene sia a livello politico (da parte dei gruppi consiliari e dei relativi uffici di supporto), sia a livello amministrativo (da parte degli organi del comune, deputati all'istruttoria e alla verifica dei requisiti soggettivi e oggettivi). Il trattamento e' altresi' finalizzato all'accertamento dei requisiti di professionalita' ed onorabilita' dei candidati alle nomine presso enti, aziende e istituzioni. Le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 32 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 18.08.2000, n. 267 (artt. 55 e ss.) - L. 25.03.1993, n. 81 - L. 30.04.1999, n. 120 - L. 5.07.1982, n. 441 - D.P.R. 16.05.1960, n. 570 - L. 19.03.1990, n. 55 (art. 15) - L. 14.04.1982, n. 164
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 32 - Sistema informativo relativo agli organi istituzionali dell'ente - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rivelare la vita sessuale (soltanto in caso di eventuale rettificazione di attribuzione di sesso)
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 32 - Trattamento effettuato per finalita' relative all'applicazione della disciplina in materia di elettorato attivo e passivo, esercizio del mandato degli organi

copia informatica per consultazione

	rappresentativi e di affidamento di incarichi di rappresentanza in enti, aziende e istituzioni nonche' accertamento dei requisiti di onorabilita' e di professionalita' per le nomine a cariche direttive di persone giuridiche. Finalita' ulteriore rispetto a quella per la quale sono raccolti i dati: pagamento emolumenti agli amministratori
Rilevanti finalita' di interesse pubblico	- Scheda n. 32 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: esercizio del mandato degli organi rappresentativi, ivicompresa la loro sospensione o il loro scioglimento, nonche' l'accertamento delle cause di ineleggibilita', incompatibilita' o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche (art. 2-sexies, comma 2 lett. g) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (applicazione della disciplina in materia di elettorato attivo e passivo, esercizio del mandato degli organi rappresentativi e di affidamento di incarichi di rappresentanza in enti, aziende e istituzioni nonche' accertamento dei requisiti di onorabilita' e di professionalita' per le nomine a cariche direttive di persone giuridiche, e pagamento emolumenti agli amministratori)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 32 - Ministero economia e finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n.164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600) e al Ministero dell'Interno per l'anagrafe degli amministratori locali (ex art. 76 d.lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa):imitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio delle decisioni in materia di candidabilita' (D.Lgs. n. 267/2000) e di anagrafe degli amministratori locali (D.Lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Amministratori
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

dati	
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza

copia informatica per consultazione

	di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks

copia informatica per consultazione

indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare
  3 = alto = = e' **probabile** che la minaccia si possa verificare
  4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da

copia informatica per consultazione

un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le

copia informatica per consultazione

	procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

copia informatica per consultazione

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomine e affidamenti incarichi per prestazioni o servizi per i quali le determinazioni siano fondate su rapporti fiduciari

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	GIUNTA COMUNALE
SERVIZIO	Giunta comunale

TRATTAMENTO	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

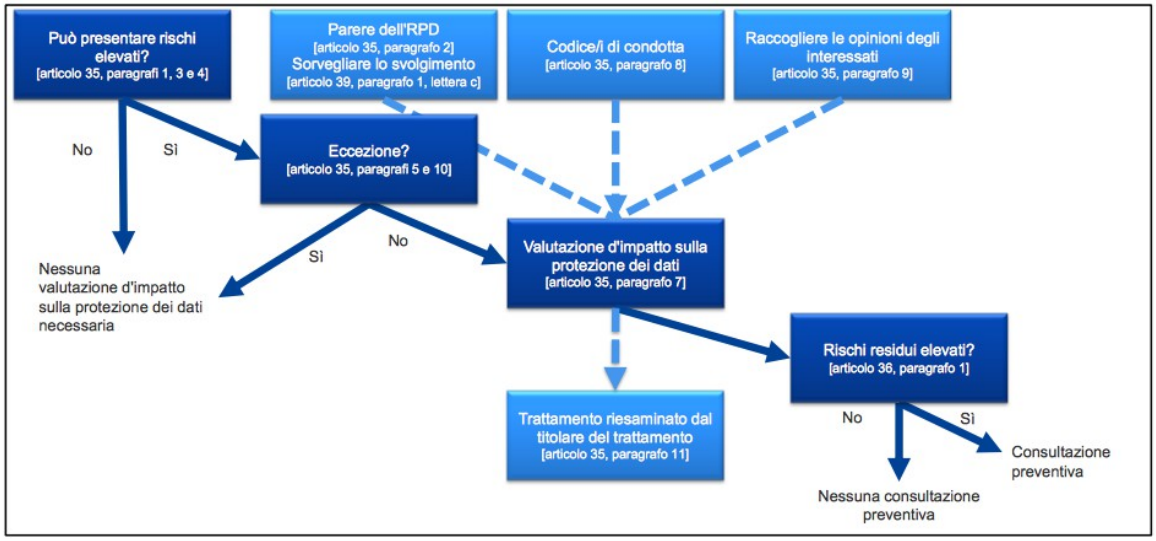
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

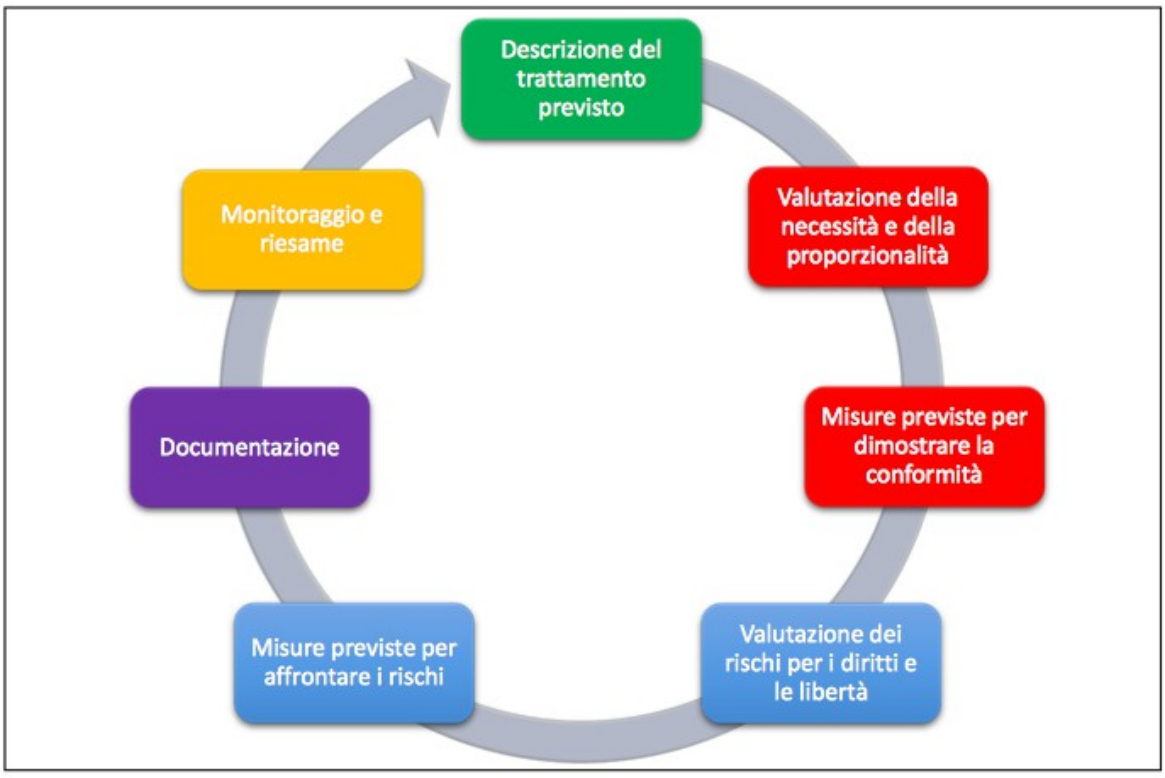
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	GIUNTA COMUNALE
SERVIZIO: denominazione e punti di contatto	Giunta comunale
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 37 - I dati vengono raccolti presso gli interessati i quali possono richiedere, per particolari iniziative, il patrocinio e/o l'erogazione di un contributo economico e/o la collaborazione dell'Amministrazione Comunale. Al fine di valutare eventuali cause ostative all'erogazione di un contributo, viene acquisita la posizione debitoria con una dichiarazione sostitutiva ai sensi degli artt. 46 e 47 del D.P.R. 445/2000. Altri dati sensibili possono emergere dagli Statuti delle associazioni, enti, fondazioni. Queste informazioni, eccetto quelle idonee a rivelare lo stato di salute, possono inoltre essere diffuse ai sensi del D.Lgs. n.267/2000 in ottemperanza al regime di pubblicita' degli atti (pubblicazioni Albo Pretorio). Con riferimento alle attivita' relative alla concessione di benefici, al riconoscimento di benefici il trattamento di dati sensibili si rende necessario sia per la concessione o l'assegnazione stesse, sia per la predisposizione delle graduatorie dei beneficiari, che vengono rese pubbliche ove previsto dalla relativa normativa, fermo restando il divieto di diffondere i dati sulla salute ai sensi degli artt. 22, comma 8, e 68, comma 3, del d.lgs. n. 196/2003. I dati vengono forniti direttamente dagli interessati, che presentano apposita domanda di contributo al Comune, oppure da terzi (anagrafe, autorita' giudiziaria, ASL, provincia, altri servizi comunali, i quali effettuano dei servizi di sostegno in favore dell'utente che versa in stato di indigenza).
Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente

copia informatica per consultazione

all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 37 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 3/3/1951, n.178; art.12 L.241/90; Regolamenti comunali in materia
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 37 - Sistema informativo relativo a concessione di onorificenze, ricompense, contributi, sussidi e benefici - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rivelare lo stato di disabilita'
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella

copia informatica per consultazione

	MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 37 - Trattamento effettuato per finalita' di diritti sociali, politiche sociali e famiglia. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 37 - Trattamento effettuato per rilevanti finalita' nella seguente materia: conferimento di onorificenze e ricompense, riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali ai sensi dell'art. 2-sexies, comma 2 lett. n) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 37 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): istanti, beneficiari (ai sensi del Regolamento per la concessione di contributi e delle normative nello stesso richiamate)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti -	

copia informatica per consultazione

particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Persone disabili - Persone fisiche - Persone in cerca di occupazione - Soggetti in difficolta' o pericolo (anche potenziali) - Soggetti con limitata capacita' di intendere e volere - Scolari o studenti di ogni ordine e grado - Rifugiati
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione	- I dati sono conservati in una forma che consente l'identificazione dell'interessato

copia informatica per consultazione

trattamento: *Periodo di conservazione dei dati*	per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia

copia informatica per consultazione

	effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita'***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei

copia informatica per consultazione

dei dati (rilevati dalla prospettiva degli interessati)	software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI

copia informatica per consultazione

	AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I

copia informatica per consultazione

	MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi,	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli

copia informatica per consultazione

modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

copia informatica per consultazione

- **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le

copia informatica per consultazione

	circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

copia informatica per consultazione

l'applicazione delle misure	

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessioni discrezionali non vincolate di contributi, benefici, esoneri e sovvenzioni (Provvedimenti amministrativi discrezionali nell'an e nel contenuto)

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	GIUNTA COMUNALE
SERVIZIO	Giunta comunale

TRATTAMENTO	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

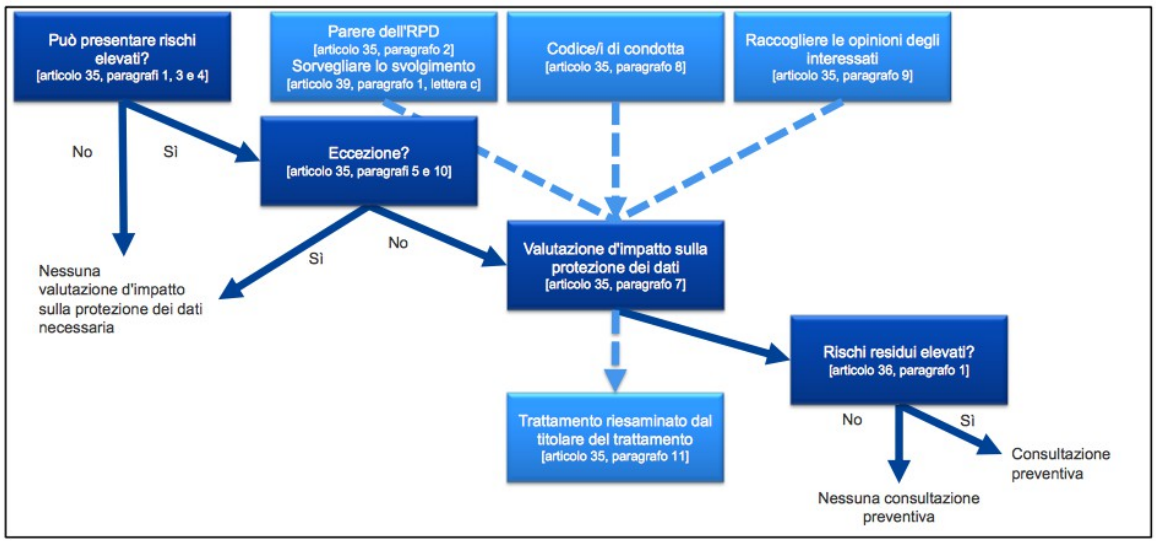
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

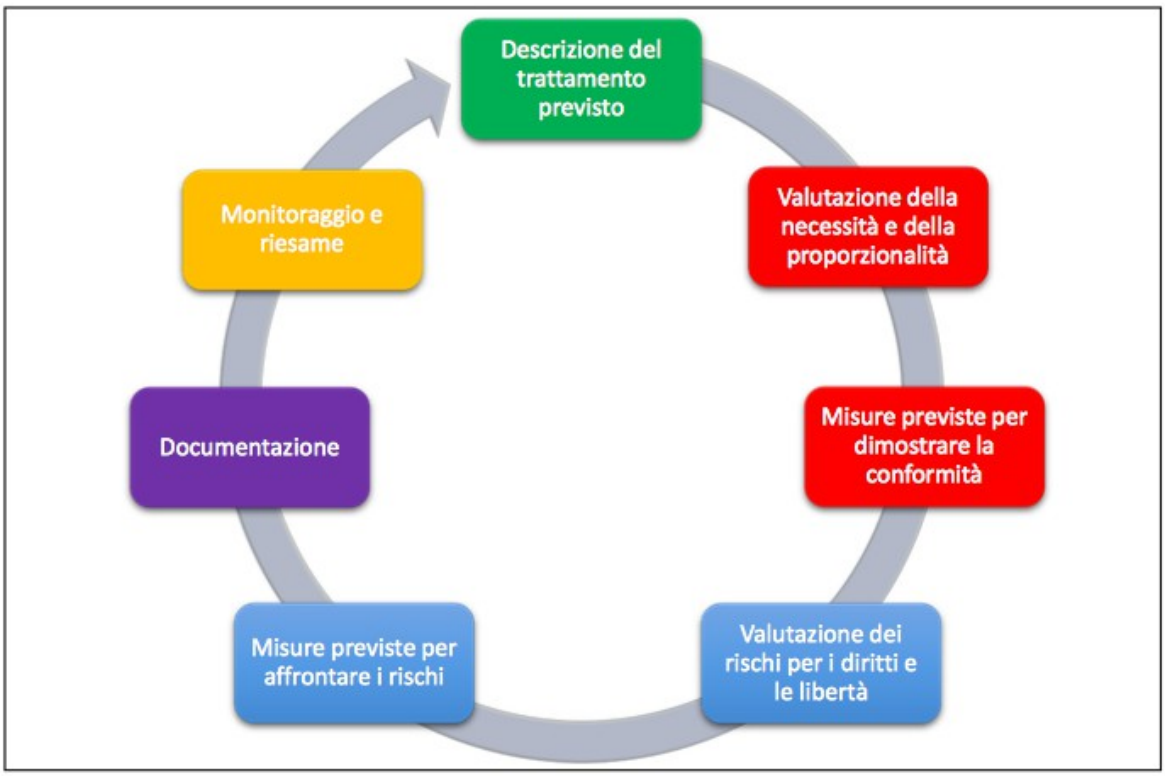
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	GIUNTA COMUNALE
SERVIZIO: denominazione e punti di contatto	Giunta comunale
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 49 - I dati vengono raccolti per la conclusione di transazioni e per la gestione di lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento. Particolari forme di elaborazione tramite interconnessione e raffronto dati con altri soggetti pubblici o privati: amministrazioni certificanti ai sensi del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 49 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento

copia informatica per consultazione

	dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo - Codice Civile - Codice procedura Civile
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 49 - Sistema informativo relativo a beni immobili, demaniali e patrimoniali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare la posizione di beni, strumenti, oggetti
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 49 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 49 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita' di lasciti e transazioni nonche' donazioni e del buon andamento,

copia informatica per consultazione

	dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 49 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) altre amministrazioni e soggetti privati (ai sensi del Regolamento sulla disciplina dei contratti, del Regolamento di contabilita' e della normativa dagli stessi richiamata)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di*	

copia informatica per consultazione

ubicazione del/i server	
Categorie di interessati	- Persone fisiche - Persone giuridiche ed altri enti (comprende societa' di persone)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III

copia informatica per consultazione

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete

copia informatica per consultazione

	internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli	Alto

copia informatica per consultazione

interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

copia informatica per consultazione

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza:	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da	

copia informatica per consultazione

tecniche informatiche, comprese le misure di ripristino in caso di data breach	consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di

copia informatica per consultazione

	ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Convenzioni, transazioni ed ogni disposizione patrimoniale di straordinaria amministrazione

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	GIUNTA COMUNALE
SERVIZIO	Giunta comunale

TRATTAMENTO	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

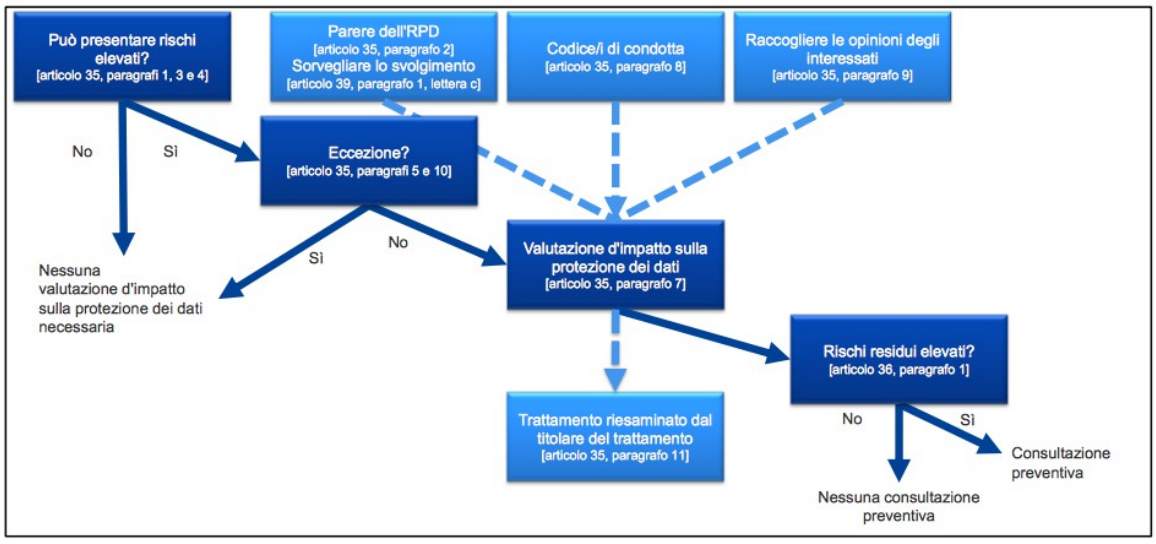
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

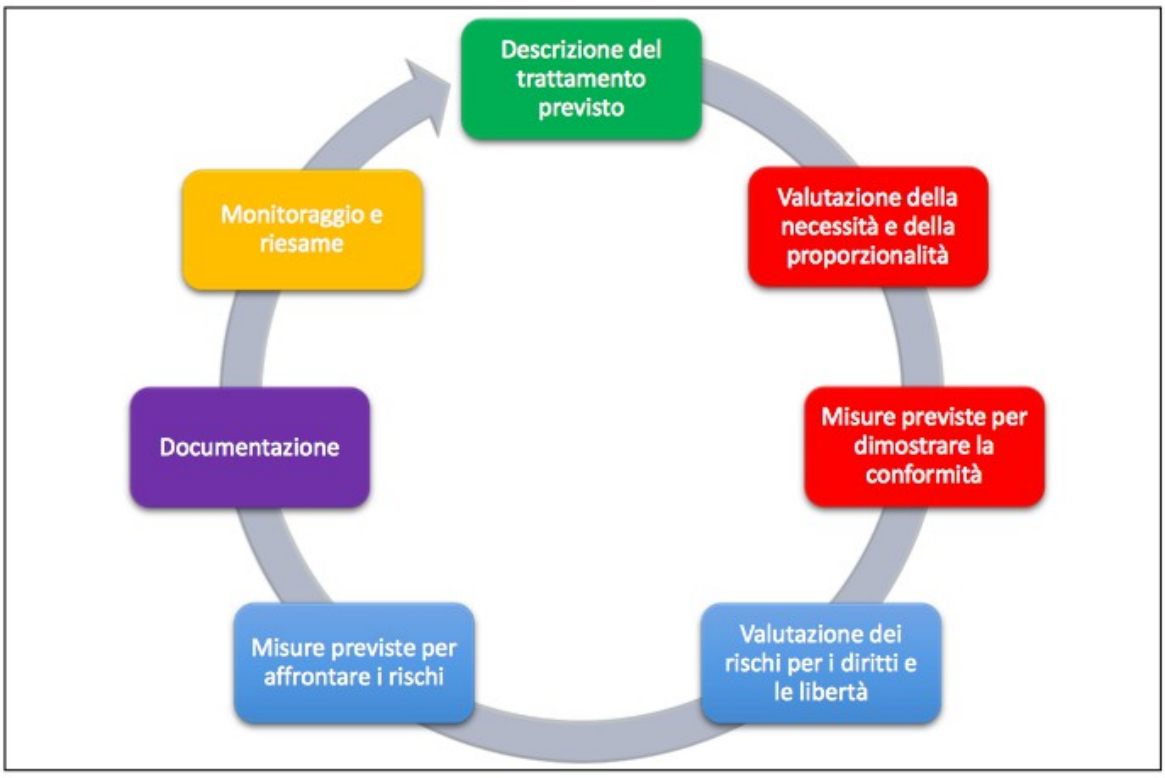
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	GIUNTA COMUNALE
SERVIZIO: denominazione e punti di contatto	Giunta comunale
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 50 - Il trattamento ha per oggetto i dati delle procedure di affidamento e dei contratti di appalto e di concessione delle amministrazioni aggiudicatrici e degli enti aggiudicatori per l'acquisizione di servizi, forniture, lavori e opere, nonche' i concorsi pubblici di progettazione e l'attivita' posta in essere in attuazione del D.Lgs. n. 50/2016. I dati vengono raccolti dai soggetti partecipanti alle procedure di affidamento e includono dati sensibili e giudiziari. Il trattamento implica, oltre alle ordinarie forme di elaborazione standardizzate (con mezzi elettronici e su supporto cartaceo), anche la comunicazione a terzi e, in particolare, alle Autorita' competenti a rilasciare le certificazioni sul possesso dei requisiti, nonche' la possibile diffusione mediante pubblicazione sul profilo del committente e sui siti web prescritti dalla normativa vigente in materia.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Fonte normativa	- Scheda n. 50 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001- Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 50/2016 - Linee Guida Anac - Statuto - Regolamento sul procedimento amministrativo - Regolamento sull'attivita' contrattuale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza trasversalmente, di tutti gli uffici che aggiudicano contratti inclusi nell'ambito di applicazione del D.Lgs. 50 n. 0/2016
Nome archivio/Banca dati	- Scheda n. 50 - Sistema informativo relativo ad appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili - Dati relativi al comportamento debitorio - Dati relativi all'affidabilita' o puntualita' nei pagamenti - Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati relativi all'adempimento di obbligazioni - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti - Dati relativi all'affidabilita' nell'esecuzione dei contratti pubblici
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del	- Scheda n. 50 - Trattamento effettuato per finalita' di adempimento di obblighi

copia informatica per consultazione

trattamento	contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 50 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 50 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Agenzia Entrate, Prefettura, Tribunale, Procura presso il Tribunale, Provincia e altri enti pubblici - INPS/INAIL/ANAC - , anche attraverso la consultazione delle relative Banche dati, per i controlli sul possesso dei requisiti dichiarati in sede di procedura di affidamento; b) altri soggetti partecipanti alla procedura di affidamento; c) consulenti e soggetti, pubblici o privati, che effettuano servizi di committenza ausiliaria; d) avvocati incaricati dell'eventuale contenzioso (ai sensi del D.Lgs. n. 50/2016 e della regolazione attuativa)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione sul sito web, in "Amministratrazione trasparente" in attuazione di obblighi di pubblicazione di cui al D. Lgs. n. 33/2013 - Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base

copia informatica per consultazione

	normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: ***trasferimento all'estero***	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Concorrenti alle procedure di affidamento di contratti pubblici - Soggetti terzi rispetto ai concorrenti, i cui dati rilevano nella procedura di affidamento
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD

copia informatica per consultazione

(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli

copia informatica per consultazione

	atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento

copia informatica per consultazione

rischi: ***accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale

copia informatica per consultazione

	Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON

copia informatica per consultazione

	AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare

copia informatica per consultazione

- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

- La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

-

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del	

copia informatica per consultazione

	trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Convenzioni con associazioni e altri enti di diritto privato non di competenza del Consiglio

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	01 - SEGRETARIO COMUNALE
SERVIZIO	Segretario Comunale
SERVIZIO	Segretario Comunale

TRATTAMENTO	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

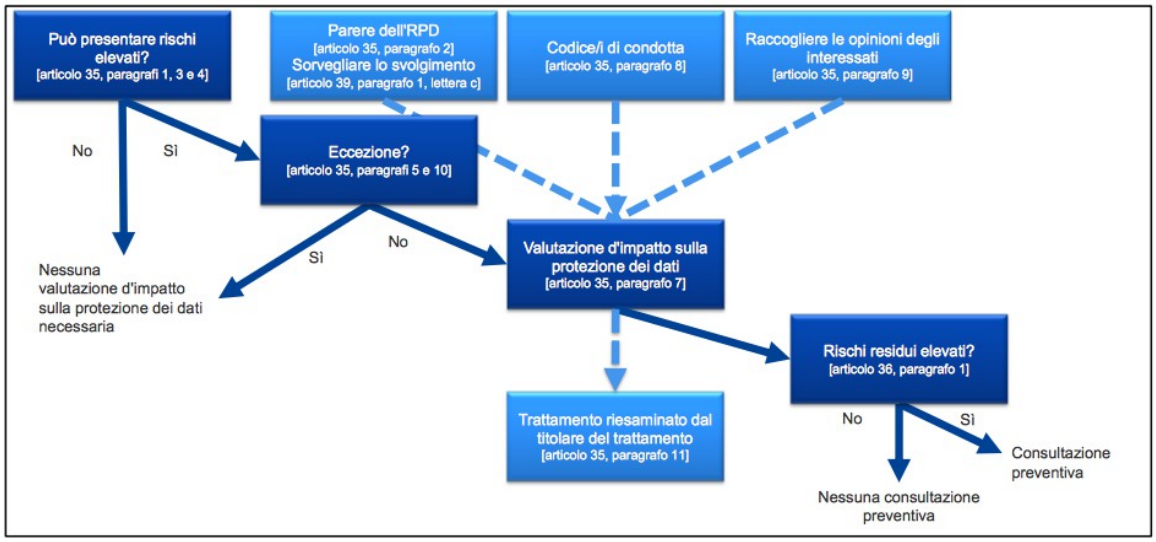
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

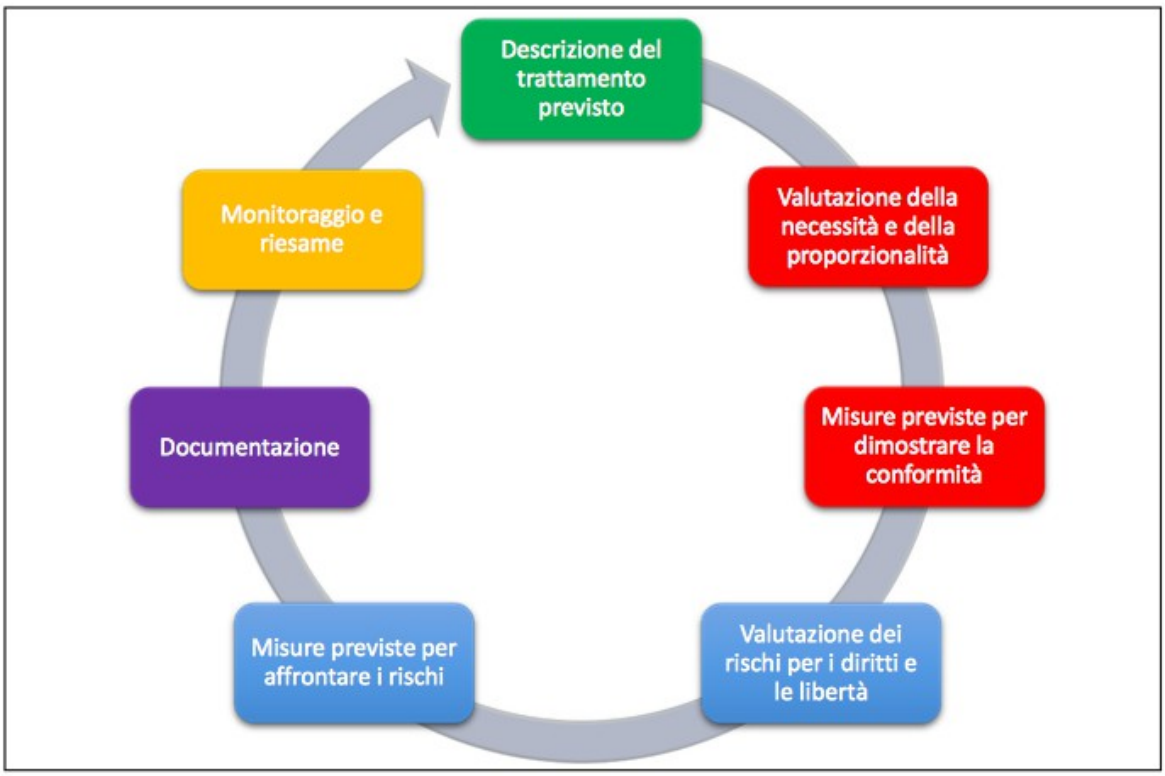
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	01 - SEGRETARIO COMUNALE
SERVIZIO	Segretario Comunale
SERVIZIO: denominazione e punti di contatto	Segretario Comunale
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 48 - Il trattamento ha per oggetto i dati relativi alla gestione del rischio di corruzione e illegalita'. I dati vengono raccolti d'ufficio, presso gli interessati e presso terzi che presentano esposti o segnalazioni. Comprende dati sensibili e giudiziari. Comporta la comunicazione a Procure (del Tribunale e Corte dei Conti) in caso di reato o danno erariale nonche' alle Autorita' di volta in volta competenti per le segnalazioni/ esposti (come, ad esempio, ANAC/AGCM). E' vietata la diffusione per essere il trattamento coperto dal segreto istruttorio salvo i casi previsti dalla L. 190/2012.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 48 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n.

copia informatica per consultazione

	123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - L. n. 179/2017 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sui controlli interni
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 48 - Sistema informativo relativo a segnalazioni illeciti, atti e documenti del sistema di gestione del rischio di corruzione e illegalita' - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 48 - Trattamento effettuato per finalita' di prevenzione del rischio di corruzione e illegalita'. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 48 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto

copia informatica per consultazione

	dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 48 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): comunicazione a Procure del Tribunale e Corte dei Conti in caso di reato o danno erariale, nonche' alle Autorita' di volta in volta competenti per le segnalazioni/ esposti come, ad esempio, ANAC/AGCM (ai sensi dell'art. 331 c.p.p. e della L.190/2012)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Segnalanti - esponenti - Soggetti terzi rispetto ai segnalanti, i cui dati rilevano nella procedura
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento:	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa

copia informatica per consultazione

modalita' di cessazione dei dati	comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati

copia informatica per consultazione

	- Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Molto alto
GRAVITA' = Y (rilevata dalla	Molto alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - livello dell'impatto, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla

copia informatica per consultazione

	protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	FRAMEWORKS FUNZIONE
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai

copia informatica per consultazione

	documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI

copia informatica per consultazione

ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Monitoraggio funzionamento PTPCT e monitoraggio singole misure

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	01 - SEGRETARIO COMUNALE
SERVIZIO	Segretario Comunale
SERVIZIO	Segretario Comunale

TRATTAMENTO	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

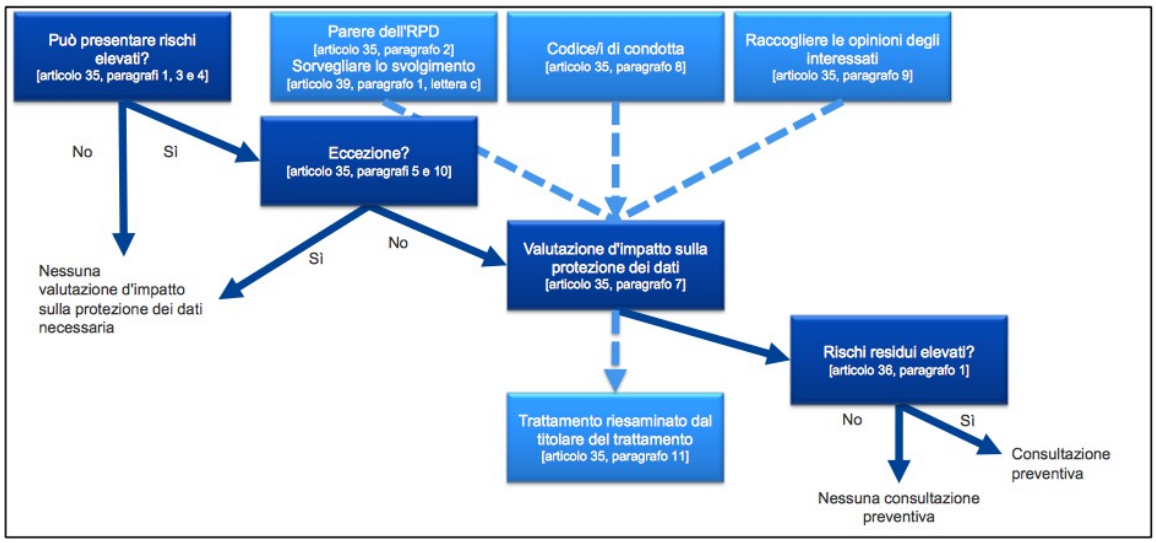
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

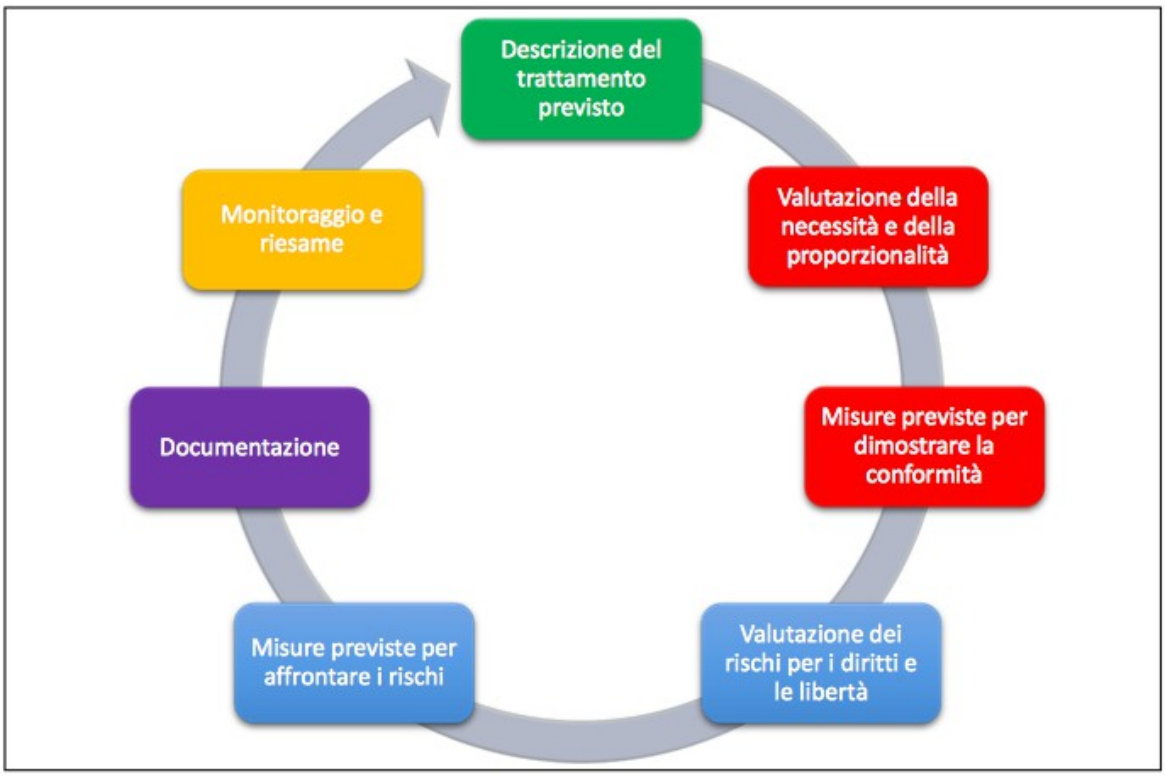
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	01 - SEGRETARIO COMUNALE
SERVIZIO	Segretario Comunale
SERVIZIO: denominazione e punti di contatto	Segretario Comunale
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 51 - I dati personali trattati nei procedimenti di accesso documentale, civico semplice e di accesso civico generalizzato vengono raccolti sia presso l'interessato che presso terzi. Il trattamento puo' includere anche dati vulnerabili. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo. In relazione ad alcuni trattamenti (quali ad esempio, l'accesso civico semplice e l'accesso civico generalizzato) vengono effettuate anche operazioni particolari di comunicazione, interconnessione e raffronti di dati (con specificazione ed indicazione della base normativa): con altri trattamenti o banche dati dello stesso ente.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 51 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 -

copia informatica per consultazione

	D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 97/2016 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sull'accesso
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 51 - Sistema informativo relativo ad accesso e trasparenza - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 51 - Trattamento effettuato per finalita' di trasparenza dell'attivita' amministrativa. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 51 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: conferimento di onorificenze e ricompense, riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto,

copia informatica per consultazione

	accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali ai sensi dell'art. 2-sexies, comma 2 lett. n) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento al riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' di rilascio e revoca di autorizzazioni o abilitazioni, di concessione di patrocini, patronati e premi di rappresentanza, di adesione a comitati d'onore e di ammissione a cerimonie ed incontri istituzionali
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 51 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): controinteressati ai sensi della L. 241/1990 e D.Lgs. 33/2013
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E. - Amministratori
Categorie di destinatari	- Soggetti privati - Soggetti pubblici - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)

copia informatica per consultazione

Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario,

copia informatica per consultazione

	aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

copia informatica per consultazione

	VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di

copia informatica per consultazione

	trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici	

copia informatica per consultazione

	MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo

copia informatica per consultazione

	livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	FRAMEWORKS FUNZIONE
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere

copia informatica per consultazione

	un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV MONITORAGGIO E RIESAME DPIA (art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

copia informatica per consultazione

Accesso art. 43, co. 2 del T.U.E.L. da parte dei consiglieri

Accesso art. 22 e segg. della L. 241/90
Accesso art. 43, co. 2 del T.U.E.L. da parte dei consiglieri

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	01 - SEGRETARIO COMUNALE
SERVIZIO	Segretario Comunale
SERVIZIO	Segretario Comunale

TRATTAMENTO	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

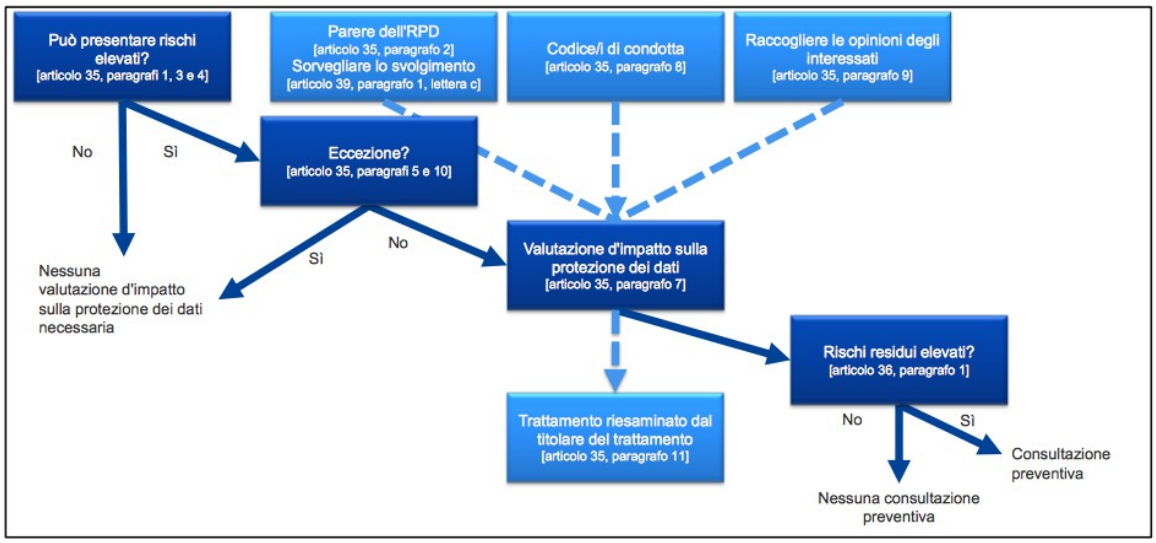
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

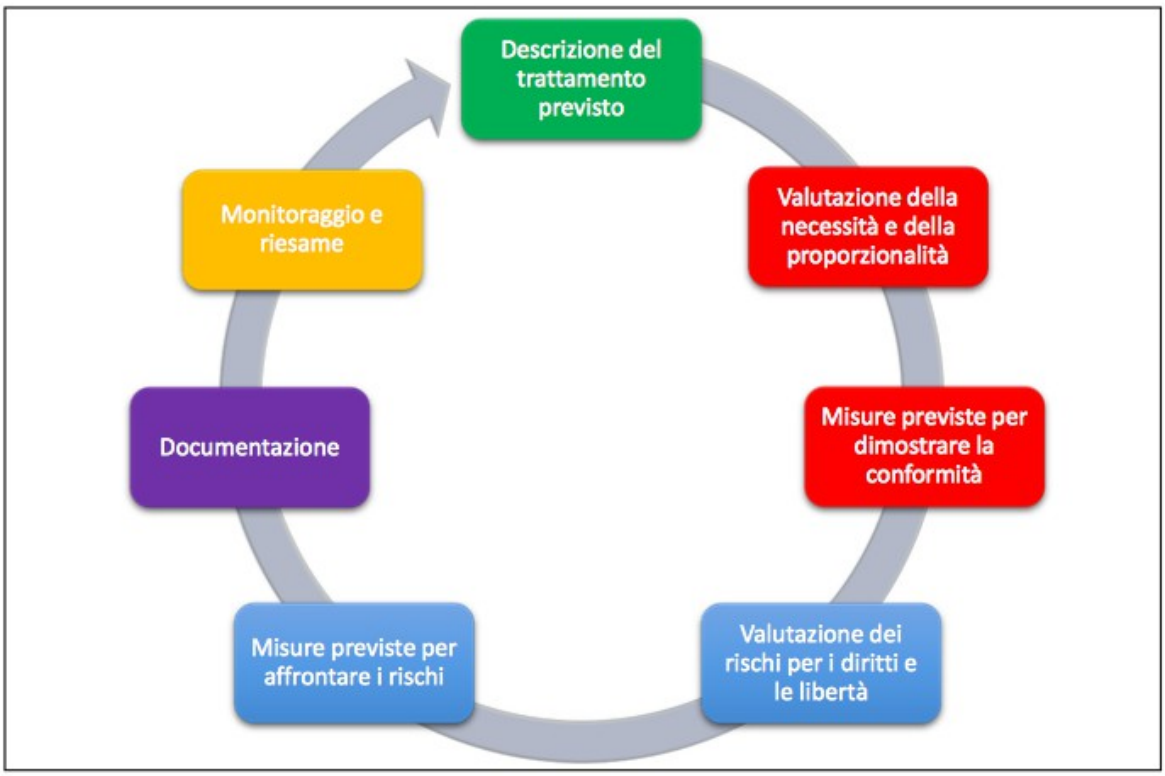
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	01 - SEGRETARIO COMUNALE
SERVIZIO	Segretario Comunale
SERVIZIO: denominazione e punti di contatto	Segretario Comunale
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto Dott. Tacchella Stefano

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 60 - I dati vengono raccolti sia presso l'ente, sia presso terzi, sia presso gli interessati (concorrenti alle procedure di affidamento di contratti pubblici) al fine della stipulazione dei contratti. Il trattamento puo' includere anche dati vulnerabili e sensibili. Basti pensare che prima di procedere alla stipulazione dei contratti l'amministrazione deve verificare in capo al contraente il possesso dei requisiti per la stipulazione con la P.a., e tra queste informazioni rientrano pure i dati giudiziari. Non solo. Anche lo stesso contenuto contrattuale puo' riguardare il trattamento di dati sensibili o giudiziari. Vengono effettuate operazioni ordinarie di elaborazione, sia con mezzi elettronici che su supporto cartaceo tramite sistema informativo, di appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n.114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 60 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art.

copia informatica per consultazione

	1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice Civile e di procedura civile
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 60 - Sistema informativo relativo alla gestione rapporti contrattuali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 60 - Trattamento effettuato per finalita' di adempimento di obblighi contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 60 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: volgimento delle funzioni di controllo, indirizzo politico,inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n.

copia informatica per consultazione

	101/2018 (verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 60 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) soggetti privati e pubblici (D.Lgs. 267/2000 - Codice di procedura civile)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i*	

copia informatica per consultazione

server	
Categorie di interessati	- Concorrenti alle procedure di affidamento di contratti pubblici
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla

copia informatica per consultazione

	protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	FRAMEWORKS FUNZIONE
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai

copia informatica per consultazione

	documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI

copia informatica per consultazione

ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rogito atti segretario comunale
Autenticazione scritture private
Trascrizione decreti esproprio e altri
Liquidazione diritti di segreteria
Registrazione contratti
Adempimenti conseguenti alla stipula del contratto: registrazione anni successivi

21

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	01 - SEGRETARIO COMUNALE
SERVIZIO	Segretario Comunale
SERVIZIO	Segretario Comunale

TRATTAMENTO	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

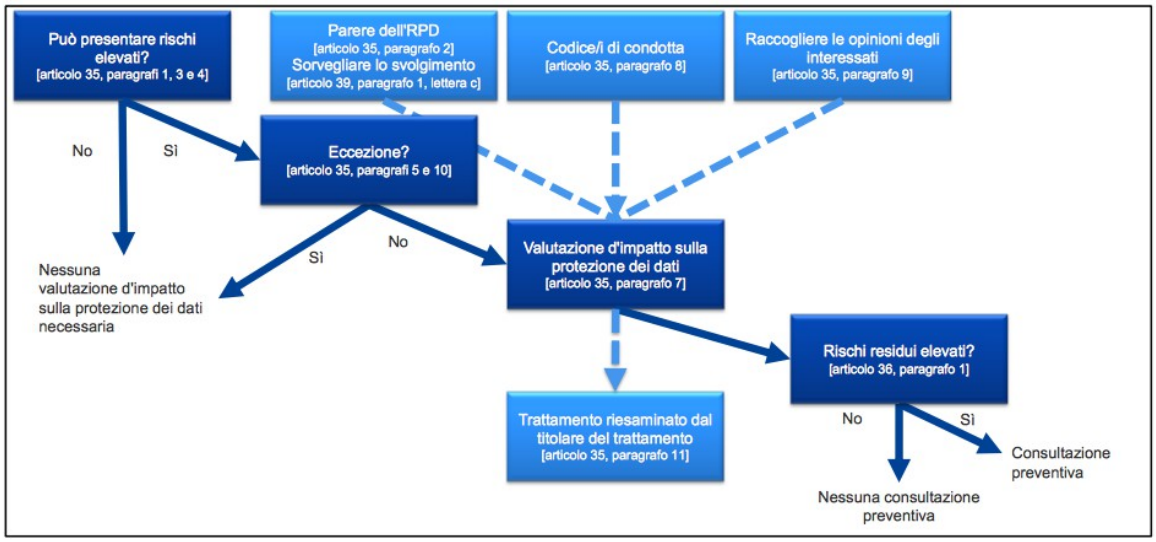
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

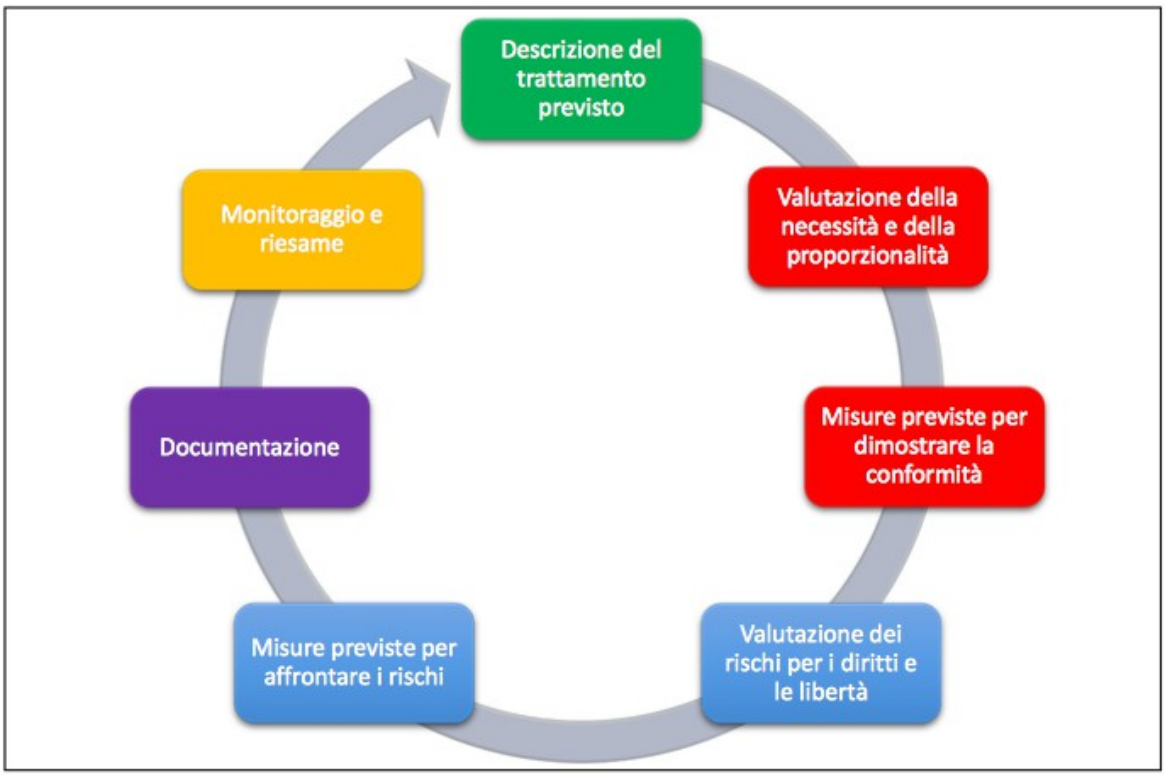
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	01 - SEGRETARIO COMUNALE
SERVIZIO	Segretario Comunale
SERVIZIO: denominazione e punti di contatto	Segretario Comunale
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig.ra Raino' Chiara Sig.ra Rossi Carla

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 61 - I dati vengono raccolti dall'Ufficio Segreteria e protocollo sia presso l'ente, sia presso terzi, sia presso gli interessati. Il trattamento (che include anche dati vulnerabili e sensibili) e' effettuato per rilevanti finalita' di interesse pubblico relative verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo tramite sistema informativo, protocollo interno, raccolta pratiche, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n.114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 61 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000

copia informatica per consultazione

	- D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 61 - Sistema informativo relativo al protocollo interno e raccolta pratiche - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 61 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 61 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: volgimento delle funzioni di controllo, indirizzo politico,inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di

copia informatica per consultazione

	razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	

copia informatica per consultazione

Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto

copia informatica per consultazione

Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla

copia informatica per consultazione

	protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	FRAMEWORKS FUNZIONE
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai

copia informatica per consultazione

	documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI

copia informatica per consultazione

ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione e archiviazione dei contratti pubblici

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZI LEGALI
SERVIZIO	Servizi Legali

TRATTAMENTO	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

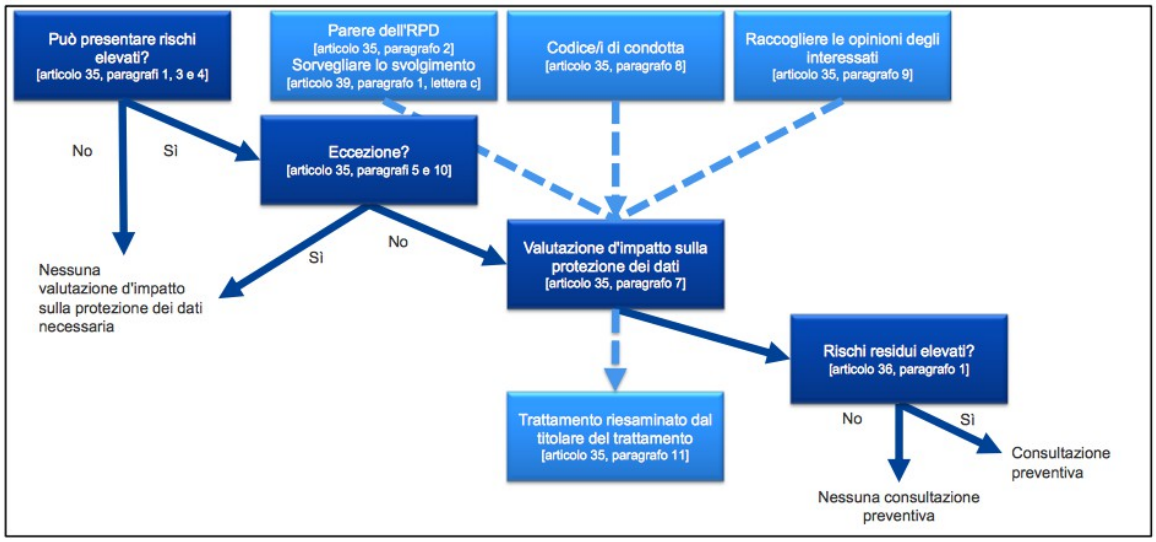
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

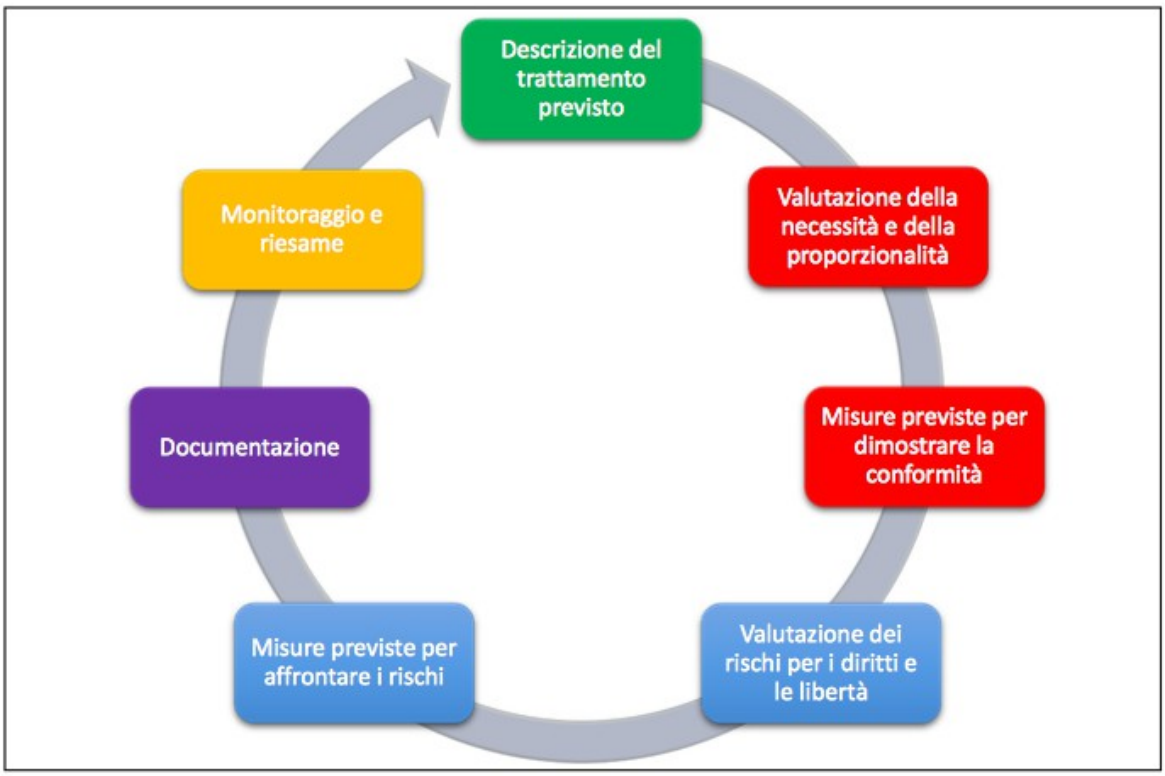
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZI LEGALI
SERVIZIO: denominazione e punti di contatto	Servizi Legali
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Organismo Indipendente di Valutazione/Componente - Presidente Nucleo di Valutazione Maggioli s.p.a.
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Dott.ssa Galli M. Cristina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 01 - Il trattamento concerne tutti i dati relativi all'instaurazione ed alla gestione del rapporto di lavoro, avviato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'ente ovvero in aziende o istituzioni collegate o vigilate, a partire dai procedimenti concorsuali o da altre procedure di selezione. I dati sono oggetto di trattamento presso le competenti strutture del Comune per quanto riguarda la gestione dell'orario di servizio, le certificazioni di malattie ed altri giustificativi delle assenze; vengono inoltre effettuati trattamenti a fini statistici e di controllo di gestione. I dati sulle convinzioni religiose possono rendersi necessari per la concessione di permessi per quelle festivita' la cui fruizione e' connessa all'appartenenza a determinate confessioni religiose; quelli sulle opinioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza o in relazione a particolari preferenze alimentari, laddove e' previsto un servizio di mensa; le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso. Possono essere raccolti anche dati sulla salute relativi ai familiari del dipendente ai fini della concessione di benefici nei soli casi previsti dalla legge. I dati pervengono su iniziativa dei dipendenti e/o previa richiesta da parte del Comune. I dati vengono trattati ai fini dell'applicazione dei vari istituti contrattuali disciplinati dalla legge (gestione giuridica, economica, previdenziale, pensionistica, attivita' di aggiornamento e formazione). Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 01 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (artt. 2094 - 2134) - D.P.R. 30.06.1965, n. 1124 - L. 20.05.1970, n. 300 - L. 7.02.1990, n. 19 - D.Lgs. 19.09.1994, n. 626 - L. 12.03.1999, n. 68 - Legge 8.03.2000, n. 53 - D.Lgs. 18.08.2000, n. 267 - D.Lgs. 30.03.2001, n. 165 - D.Lgs. 26.03.2001, n. 151 - L. 6.03.2001, n. 64 - D.P.R. 28.12.2000, n. 445 - D.Lgs. 15.08.1991, n. 277 - L. 14.04.1982, n. 164 - CCNL - Contratto collettivo decentrato di ogni singolo ente - Regolamenti comunali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 01 - Sistema informativo relativo alla gestione rapporti contrattuali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rivelare la vita sessuale (soltanto in caso di rettificazione di sesso) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del

copia informatica per consultazione

	dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 01 - Trattamento effettuato per finalita' di gestione del rapporto di lavoro in tutte le sue fasi. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 01 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva ai sensi dell'art. 2-sexies, comma 2 lett. dd) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 01 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) alle organizzazioni sindacali ai fini della gestione dei permessi e delle trattenute sindacali relativamente ai dipendenti che hanno rilasciato delega; b) enti assistenziali, previdenziali e assicurativi e autorita' locali di pubblica sicurezza a fini assistenziali e previdenziali, nonche' per rilevazione di eventuali patologie o infortuni sul lavoro; c) alla Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (d.lgs. n. 165/2001); d) uffici competenti per il collocamento mirato, relativamente ai dati anagrafici degli assunti appartenenti alle "categorie protette"; e) strutture sanitarie competenti per le visite fiscali (art. 5, l. n.

copia informatica per consultazione

	300/1970 e CCNL); f) enti di appartenenza dei lavoratori comandati in entrata (per definire il trattamento retributivo del dipendente); g) Ministero economia e finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600); h) ISPELS (ax art. 70 d.lgs. n. 626/1994)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Personale dipendente - Collaboratori
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware,*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

software, reti, persone, supporti cartacei o canali di trasmissione	
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

copia informatica per consultazione

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati

copia informatica per consultazione

	risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di

copia informatica per consultazione

	software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;

copia informatica per consultazione

- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

- **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative	

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di

copia informatica per consultazione

	consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**

copia informatica per consultazione

art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2

copia informatica per consultazione

	- Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione dei procedimenti di segnalazione e reclamo
Supporto giuridico e pareri legali

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZI LEGALI
SERVIZIO	Servizi Legali

TRATTAMENTO	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

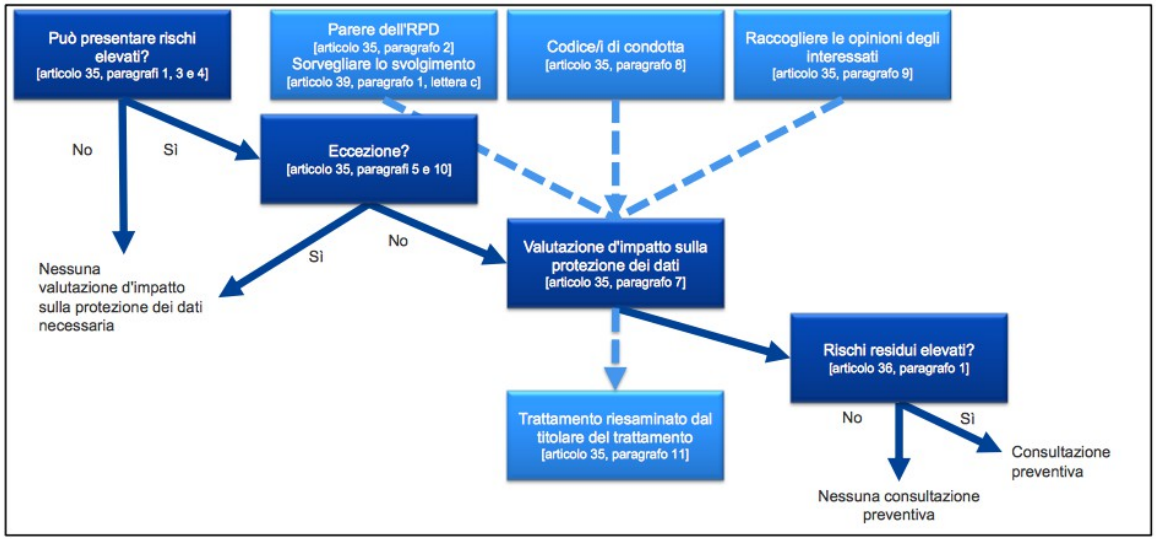
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

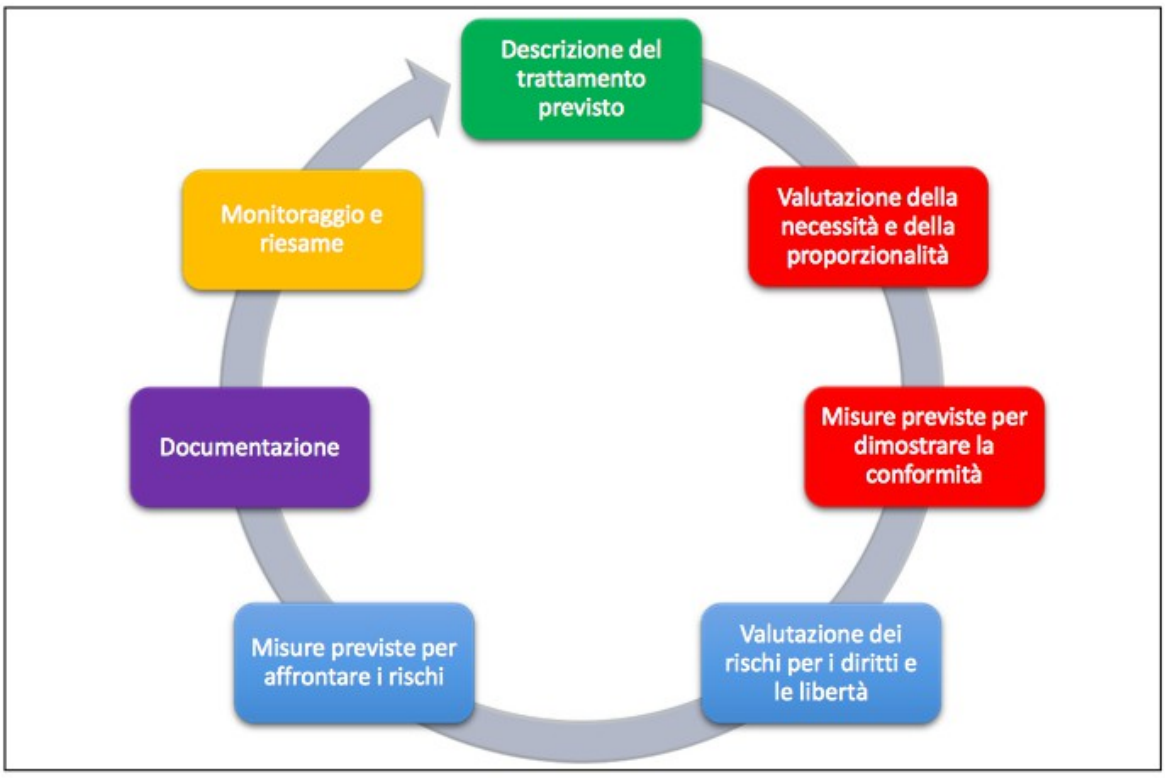
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZI LEGALI
SERVIZIO: denominazione e punti di contatto	Servizi Legali
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig.ra Lupi Claudia sig. Orzati Massimiliano sig. Cottone Pietro

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 30 - Vengono effettuate la raccolta, la consultazione e l'elaborazione dei dati nell'ambito di pareri resi all'Amministrazione, di scritti difensivi prodotti in giudizio, cosi' come nell'ambito delle richieste di indennizzo e/o danni inerenti la responsabilita' civile verso terzi dell'amministrazione. Vengono effettuati eventuali raffronti ed interconnessioni con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000. Gli stessi possono essere comunicati agli uffici competenti per la relativa trattazione amministrativa, all'Autorita' giudiziaria (che puo' anche comunicarli all'ente), al professionista per un'eventuale attribuzione di incarico; agli Enti previdenziali (Inail, Inps, Inpdap),agli enti di patronato ed ai sindacati (incaricati di indagini difensive proprie e altrui); alle societa' di riscossione tributi/sanzioni, nonche' al consulente della controparte e al consulente nominato dall'Autorita' giudiziaria (per le finalita' di corrispondenza sia in fase pregiudiziale, sia in corso di causa, nonche' per la gestione dei sinistri causati direttamente o indirettamente a terzi). I dati riguardano ogni fattispecie che possa dare luogo ad un contenzioso.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 30 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile - Codice penale - Codice di procedura civile - Codice di procedura penale - Leggi sulla giustizia amministrativa (fra le altre: R.D. 17.08.1907, n. 642; R.D. 26.06.1924, n. 1054; R.D. 12.07.1934, n. 1214; L. 6.12.1971, n. 1034; L. 14.11.1994, n. 19) - D.Lgs. 18.08.2000, n. 267 - D.Lgs. 30.03.2001, n. 165 - D.P.R. 29.10.2001, n. 461
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 30 - Sistema informativo relativo a pareri e consulenze - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rivelare la vita sessuale

copia informatica per consultazione

Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 30 - Trattamento effettuato per finalita' relative a: attivita' volte a fare valere il diritto di difesa in sede amministrativa o giudiziaria. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 30 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia:attivita' sanzionatorie e di tutela in sede amministrativa o giudiziaria ai sensi dell'art. 2-sexies, comma 2 lett. q) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' volte a fare valere il diritto di difesa in sede amministrativa o giudiziaria)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 30 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa: a) Autorita' giudiziaria, avvocati e consulenti tecnici incaricati dall'Autorita' giudiziaria, Enti previdenziali (Inail, Inps, Inpdap), enti di patronato, sindacati, incaricati di indagini difensive proprie e altrui, societa' di riscossione tributi/sanzioni, consulenti della controparte (per le finalita' di corrispondenza sia in fase pregiudiziale, sia in corso di causa, per la gestione dei sinistri causati direttamente o indirettamente a terzi); b) societa' assicuratrici (per la valutazione e la copertura economica degli indennizzi per la responsabilita' civile verso terzi); c) struttura sanitaria e Comitato di verifica per le cause di servizio (per la relativa trattazione amministrativa ai sensi del d.P.R. n. 461/2001); d) alle amministrazioni coinvolte nel caso in cui venga presentato il ricorso straordinario al Capo dello Stato (per la relativa trattazione, ai sensi della legge n. 1199/1971)
Categorie di	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito

copia informatica per consultazione

trattamenti - particolari forme di elaborazione: ***diffusione***	ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: ***trasferimento all'estero***	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Utenti (anche potenziali)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD

copia informatica per consultazione

(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli

copia informatica per consultazione

	atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento

copia informatica per consultazione

rischi: ***accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale

copia informatica per consultazione

	Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON

copia informatica per consultazione

	AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare

copia informatica per consultazione

- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

- La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

-

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale	

copia informatica per consultazione

	Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

	- MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e

copia informatica per consultazione

	formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Affidamento del contenzioso GdP e Tribunale alla difesa esterna mediante il sistema dell'affidamento diretto
Gestione del contenzioso

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Servizio Ambiente e Infrastrutture
SERVIZIO	Servizio Ambiente e Infrastrutture

TRATTAMENTO	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	02/03/2022
Stato del documento	Approvato dal titolare con proprio provvedimento

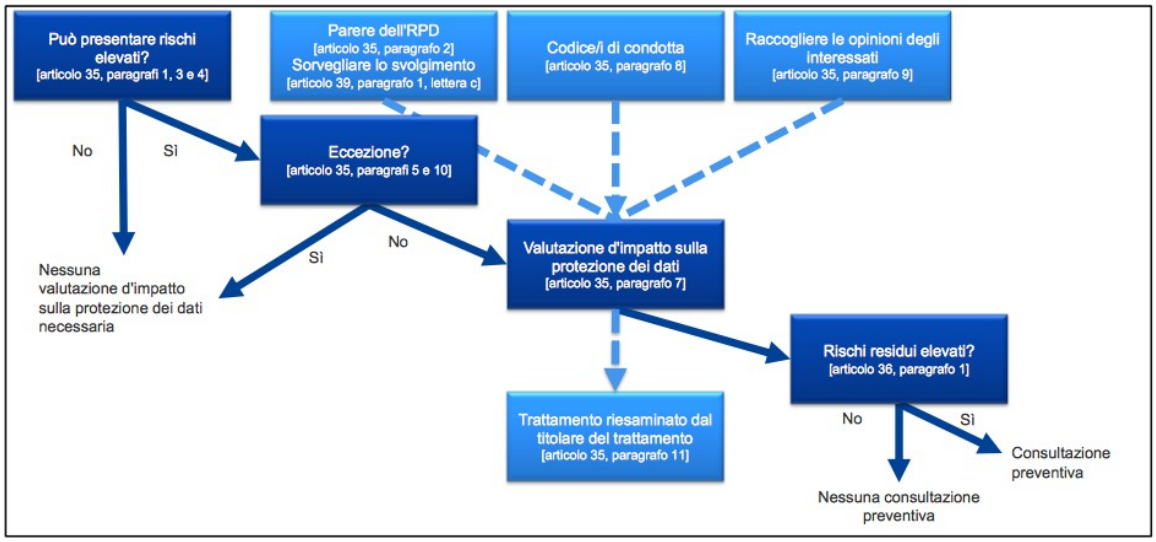
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

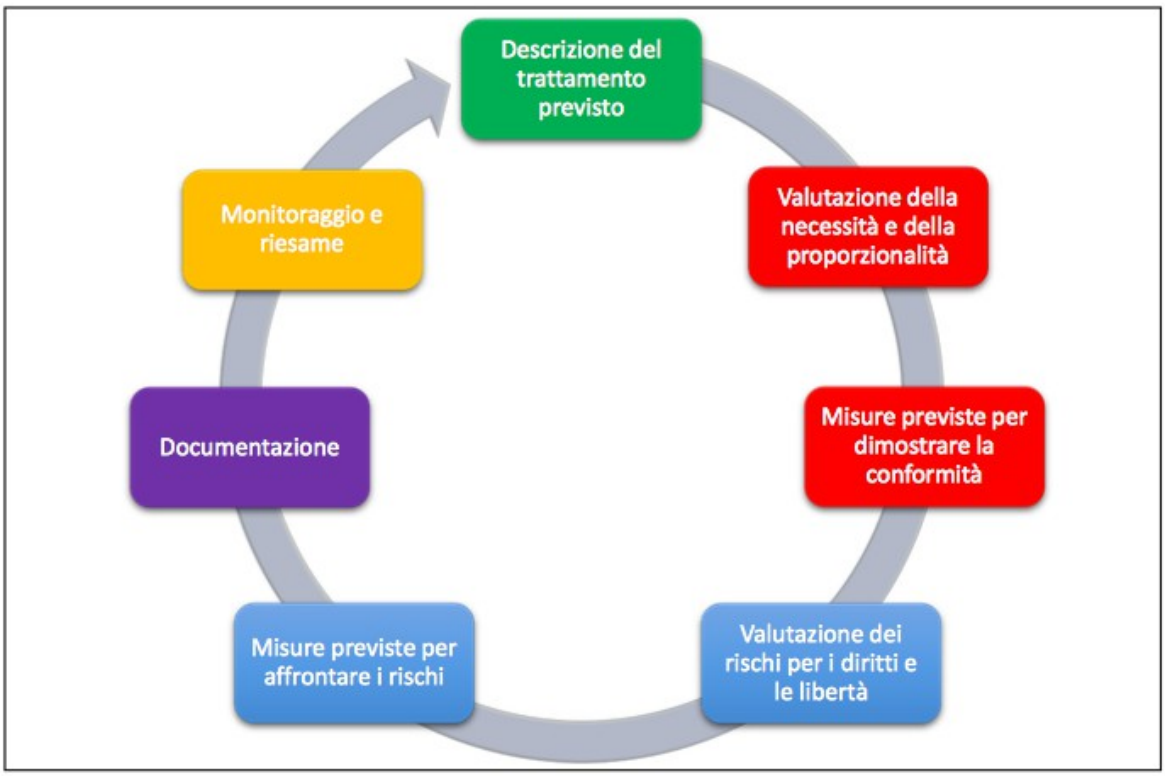
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Servizio Ambiente e Infrastrutture
SERVIZIO: denominazione e punti di contatto	Servizio Ambiente e Infrastrutture
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Soggetto affidatario del servizio di riscossione tributaria
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Arch. Braccesi Priscilla
Incaricati trattamento: denominazione e punti di contatto	

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 38 - I dati vengono raccolti sia presso l'ente, sia presso terzi, sia presso gli interessati. Il trattametno puo' includere anche dati vulnerabili e sensibili per finalita' di gestione delle entrate tributarie e servizi fiscali. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo e, in relazione ad alcuni trattamenti vengono effettuate anche operazioni particolari di elaborazione per la comunicazione ai seguenti soggetti delle suddette finalita' (con specificazione ed indicazione dell'eventuale base normativa): Agenzia Entrate; Altre pubbliche amministrazioni

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 38 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n.

copia informatica per consultazione

	123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.P.R. 380/2001 - Testo Unico delle disposizioni legislative e regolamentari in materia edilizia - Regolamento Edilizio - D.Lgs. 222/2016 - Individuazione di procedimenti oggetto di autorizzazione, SCIA, silenzio-assenso e comunicazione e di definizione dei regimi amministrativi applicabili a determinate attivita' e procedimenti - R.D. 2440/1923 - Leggi finanziarie annuali - Statuto - Regolamento sul procedimento amministrativo - D. Lgs. 504 del 30.12.1992, D. Lgs. 507 del 15.11.1993, L.R. n.96 del 20.12.1996, D.P.R. 118 del 7.04.2000
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 38 - Base di dati: sistema informativo, trattamento fiscale, contributivo e assicurativo, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 38 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: gestione delle entrate tributarie e servizi fiscali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 38 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti

copia informatica per consultazione

	riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (controllo, di indirizzo politico e di sindacato ispettivo e documentazione dell'attivita' istituzionale di organi pubblici)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 38 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Agenzia Entrate; Altre pubbliche amministrazioni (ai sensi del Regolamenti sui tributi e delle normative nello stesso richiamate)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i*	

copia informatica per consultazione

server	
Categorie di interessati	- Amministrazioni pubbliche di cui all'art. 2, co. 1, D.Lgs. 165/2001
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid

copia informatica per consultazione

	delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di

copia informatica per consultazione

	accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA'	Alto

copia informatica per consultazione

(rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - livello dell'impatto, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante

copia informatica per consultazione

	- MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**

copia informatica per consultazione

art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione Responsabile di Posizione Organizzativa individuato in base agli atti di organizzazione, competente per materia a gestire l'attivita' e il trattamento dei dati

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Tributi locali (IMU, addizionale IRPEF, ecc.)

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Servizio Ambiente e Infrastrutture
SERVIZIO	Servizio Ambiente e Infrastrutture

TRATTAMENTO	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

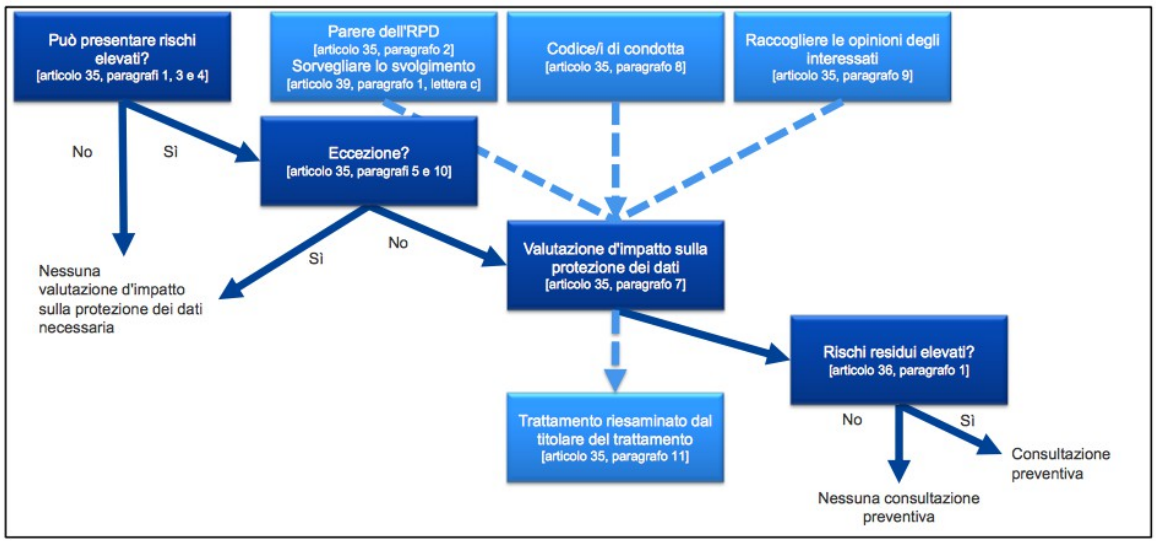
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

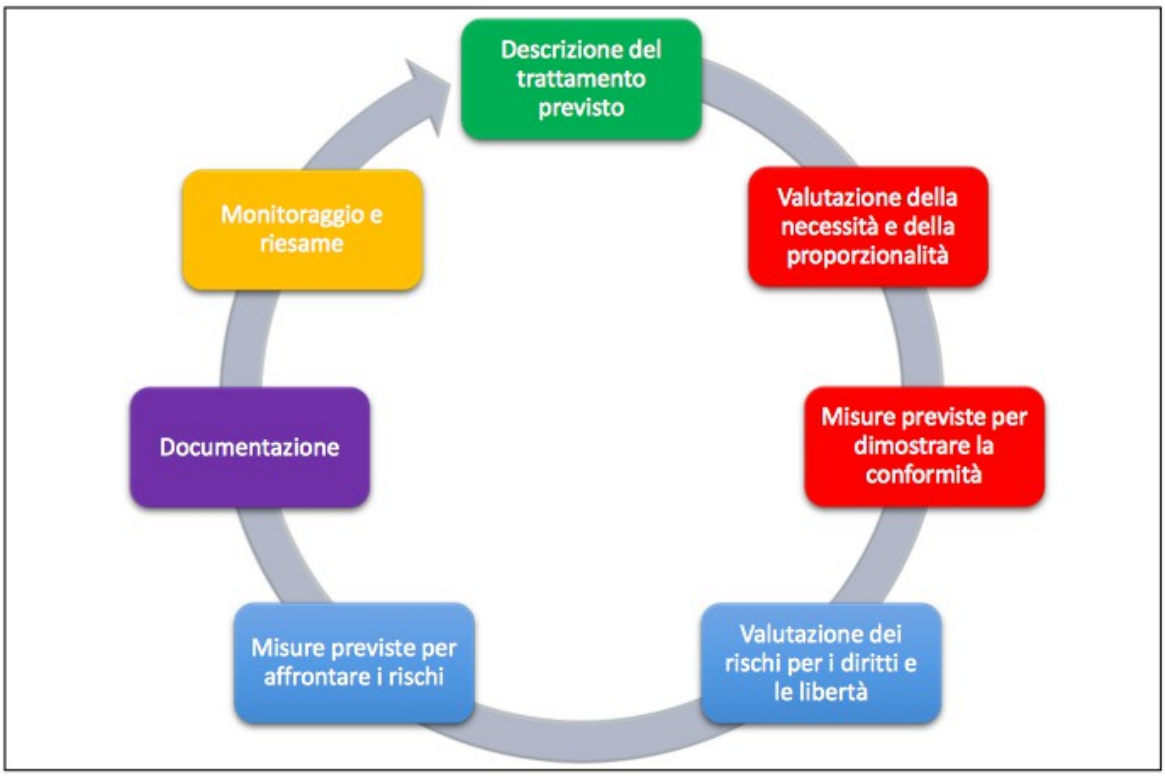
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Servizio Ambiente e Infrastrutture
SERVIZIO: denominazione e punti di contatto	Servizio Ambiente e Infrastrutture
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Arch. Braccesi Priscilla
Incaricati trattamento: denominazione e punti di contatto	sig. Cavicchioli Gaetano Dott.ssa Mazzanti Agnese sig. Corsi Francesco Dott. Dini Carlo

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 42 - I dati vengono acquisiti dagli interessati al momento del sopralluogo e dell'ispezione o verifica; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti o eventuali violazioni rispetto alle dichiarazioni acquisite. I dati sono registrati in archivi/ banche di dati gestite con modalita' elettroniche e su supporti cartacei tramite sistema informativo, controlli esterni, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 42 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000

copia informatica per consultazione

	- D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - D.Lg. n. 50/2016 - Reg. UE 679/2016 - DL. 24 novembre 1981 n. 689 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sui controlli interni
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 42 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 42 - Trattamento effettuato per attivita' di controllo, ispettive, comprese le attivita' di sopralluogo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 42 -Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di controllo, ispettive, comprese le attivita' di sopralluogo con la polizia locale)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo

copia informatica per consultazione

	interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 42 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Autorita' giudiziaria, autorita' di pubblica sicurezza (per accertamenti di carattere giudiziario); b) al RUP e alla stazione appaltante (D.Lgs. n. 50/2016); c) alle autorita' amministrative di vigilanza (D.Lgs. n. 50/2016)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Persone fisiche - Cittadini italiani - Persone giuridiche ed altri enti (comprende societa' di persone) - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.

copia informatica per consultazione

Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione

copia informatica per consultazione

Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante

copia informatica per consultazione

	- MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**

copia informatica per consultazione

art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Gestione delle Isole ecologiche

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Servizio Ambiente e Infrastrutture
SERVIZIO	Servizio Ambiente e Infrastrutture

TRATTAMENTO	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

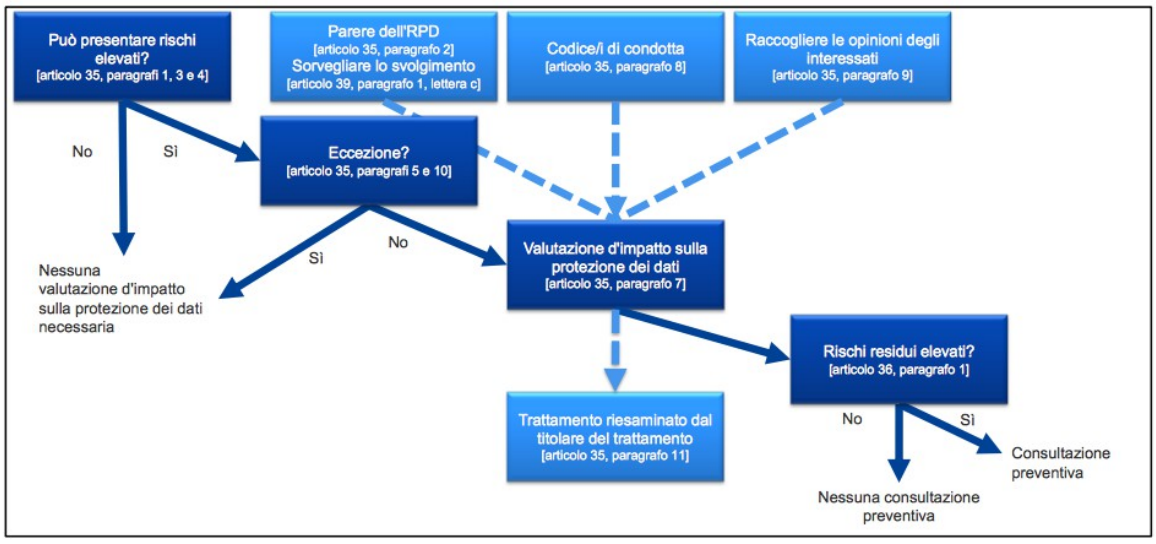
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	001
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

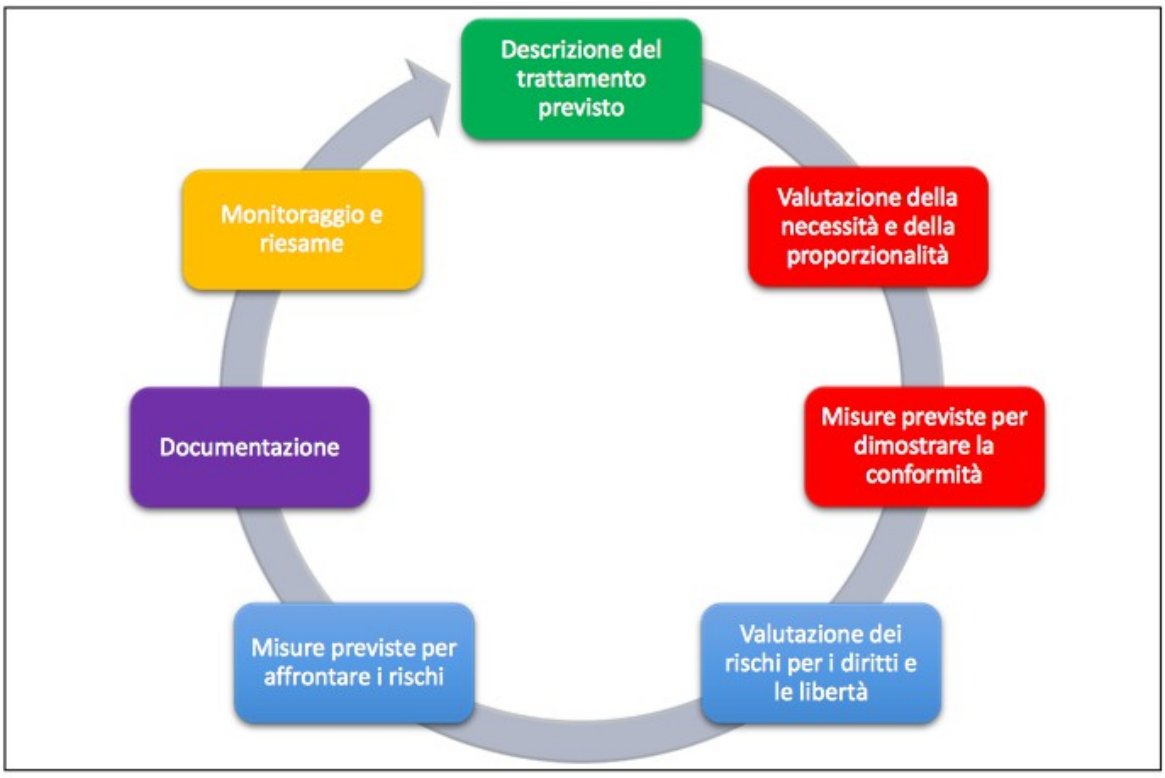
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Servizio Ambiente e Infrastrutture
SERVIZIO: denominazione e punti di contatto	Servizio Ambiente e Infrastrutture
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Arch. Braccesi Priscilla
Incaricati trattamento: denominazione e punti di contatto	sig. Cavicchioli Gaetano Dott.ssa Mazzanti Agnese sig. Corsi Francesco Dott. Dini Carlo

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 50 - Il trattamento ha per oggetto i dati delle procedure di affidamento e dei contratti di appalto e di concessione delle amministrazioni aggiudicatrici e degli enti aggiudicatori per l'acquisizione di servizi, forniture, lavori e opere, nonche' i concorsi pubblici di progettazione e l'attivita' posta in essere in attuazione del D.Lgs. n. 50/2016. I dati vengono raccolti dai soggetti partecipanti alle procedure di affidamento e includono dati sensibili e giudiziari. Il trattamento implica, oltre alle ordinarie forme di elaborazione standardizzate (con mezzi elettronici e su supporto cartaceo), anche la comunicazione a terzi e, in particolare, alle Autorita' competenti a rilasciare le certificazioni sul possesso dei requisiti, nonche' la possibile diffusione mediante pubblicazione sul profilo del committente e sui siti web prescritti dalla normativa vigente in materia.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 50 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001- Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 50/2016 - Linee Guida Anac - Statuto - Regolamento sul procedimento amministrativo - Regolamento sull'attivita' contrattuale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza trasversalmente, di tutti gli uffici che aggiudicano contratti inclusi nell'ambito di applicazione del D.Lgs. 50 n. 0/2016
Nome archivio/Banca dati	- Scheda n. 50 - Sistema informativo relativo ad appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili - Dati relativi al comportamento debitorio - Dati relativi all'affidabilita' o puntualita' nei pagamenti - Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati relativi all'adempimento di obbligazioni - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti - Dati relativi all'affidabilita' nell'esecuzione dei contratti pubblici
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi

copia informatica per consultazione

Finalita' del trattamento	- Scheda n. 50 - Trattamento effettuato per finalita' di adempimento di obblighi contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 50 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 50 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Agenzia Entrate, Prefettura, Tribunale, Procura presso il Tribunale, Provincia e altri enti pubblici - INPS/INAIL/ANAC - , anche attraverso la consultazione delle relative Banche dati, per i controlli sul possesso dei requisiti dichiarati in sede di procedura di affidamento; b) altri soggetti partecipanti alla procedura di affidamento; c) consulenti e soggetti, pubblici o privati, che effettuano servizi di committenza ausiliaria; d) avvocati incaricati dell'eventuale contenzioso (ai sensi del D.Lgs. n. 50/2016 e della regolazione attuativa)
Categorie di trattamenti - particolari forme di elaborazione:	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione sul sito web, in "Amministratrazione trasparente" in attuazione di obblighi di pubblicazione di cui al D. Lgs. n. 33/2013

copia informatica per consultazione

diffusione	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Concorrenti alle procedure di affidamento di contratti pubblici - Soggetti terzi rispetto ai concorrenti, i cui dati rilevano nella procedura di affidamento
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

cartacei o canali di trasmissione	
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- Il periodo di conservazione dei dati e' di 10 anni dall'aggiudicazione definitiva per la stazione appaltante e dalla conclusione dell'esecuzione del contratto per la Committente. I dati potranno essere conservati, anche in forma aggregata, per fini di studio o statistici nel rispetto degli artt. 89 del Regolamento UE e 110 bis del Codice Privacy
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II

copia informatica per consultazione

VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la

copia informatica per consultazione

	consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

RISCHI **Origine/fonte dei rischi:** ***accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle

copia informatica per consultazione

	password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC

copia informatica per consultazione

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

copia informatica per consultazione

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative	

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del

copia informatica per consultazione

	Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai

copia informatica per consultazione

	mutamenti di contesto

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Pulizia delle strade e delle aree pubbliche

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Bilancio
SERVIZIO	Servizio Bilancio

TRATTAMENTO	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	21/04/2020

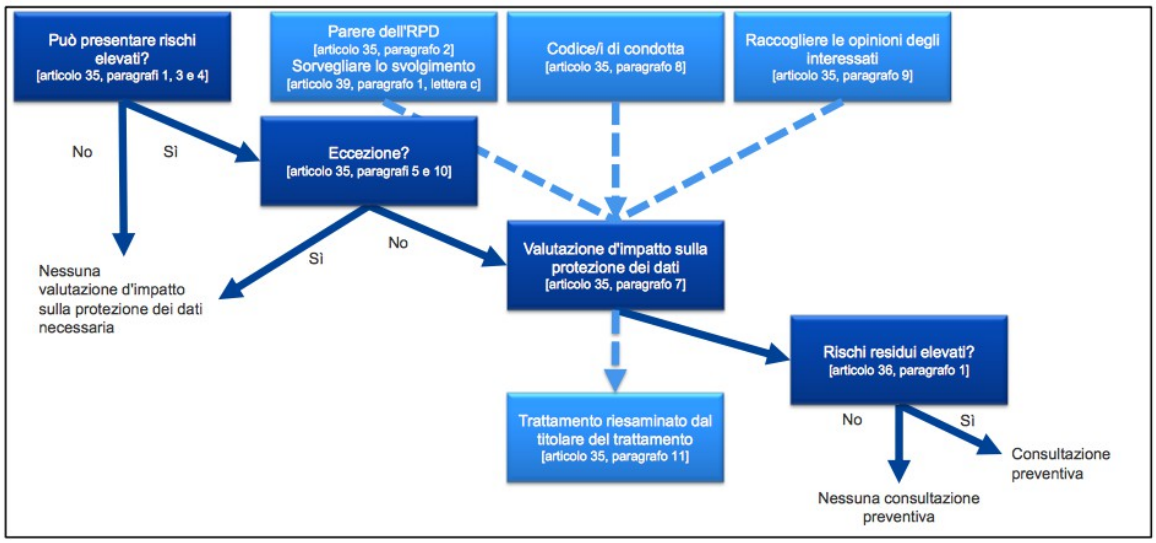
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

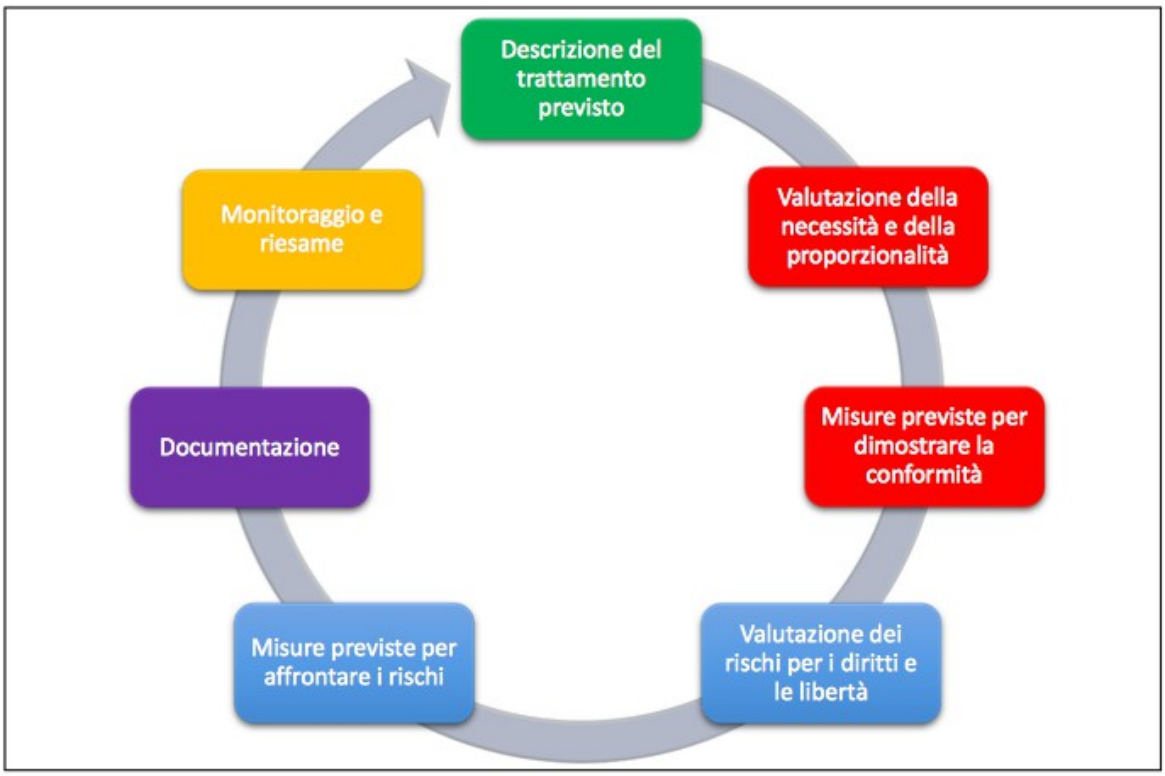
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Bilancio
SERVIZIO: denominazione e punti di contatto	Servizio Bilancio
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Servidei Stefano
Incaricati trattamento: denominazione e punti di contatto	sig. Ferrini Giampiero

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 42 - I dati vengono acquisiti dagli interessati al momento del sopralluogo e dell'ispezione o verifica; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti o eventuali violazioni rispetto alle dichiarazioni acquisite. I dati sono registrati in archivi/ banche di dati gestite con modalita' elettroniche e su supporti cartacei tramite sistema informativo, controlli esterni, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 42 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n.

copia informatica per consultazione

	123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - D.Lg. n. 50/2016 - Reg. UE 679/2016 - DL. 24 novembre 1981 n. 689 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sui controlli interni
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 42 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 42 - Trattamento effettuato per attivita' di controllo, ispettive, comprese le attivita' di sopralluogo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 42 -Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di controllo, ispettive, comprese le attivita' di sopralluogo con la polizia locale)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la

copia informatica per consultazione

	protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 42 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Autorita' giudiziaria, autorita' di pubblica sicurezza (per accertamenti di carattere giudiziario); b) al RUP e alla stazione appaltante (D.Lgs. n. 50/2016); c) alle autorita' amministrative di vigilanza (D.Lgs. n. 50/2016)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Persone fisiche - Cittadini italiani - Persone giuridiche ed altri enti (comprende societa' di persone) - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT

copia informatica per consultazione

	(amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n.

copia informatica per consultazione

approvati	62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

copia informatica per consultazione

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

copia informatica per consultazione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA'	Alto

copia informatica per consultazione

E GRAVITA' (rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a)

copia informatica per consultazione

	Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Verifiche Revisore dei Conti

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio di Protezione Civile
SERVIZIO	Servizio di Protezione Civile

TRATTAMENTO	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

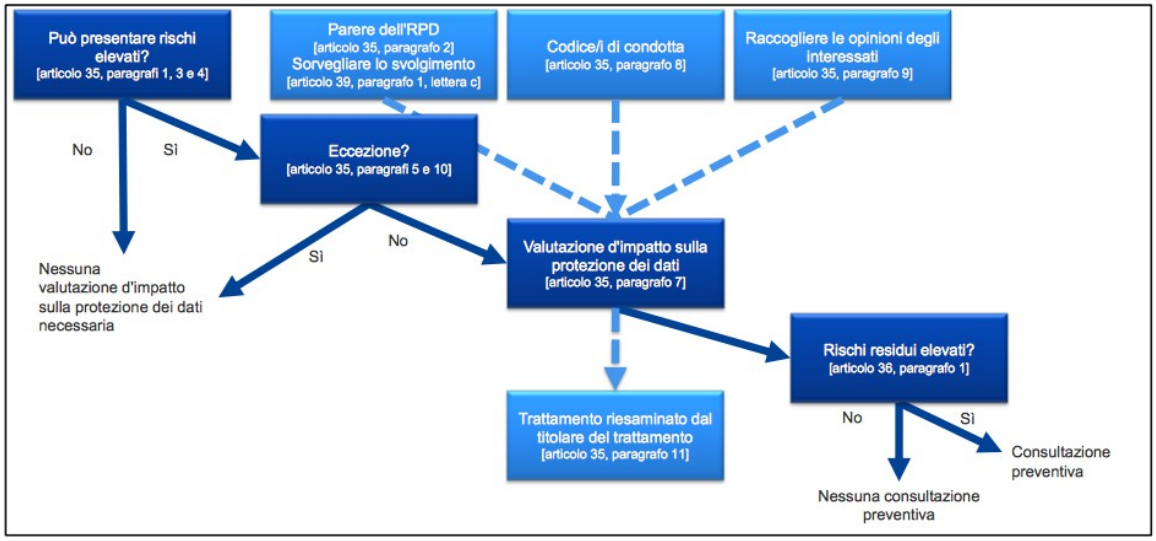
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

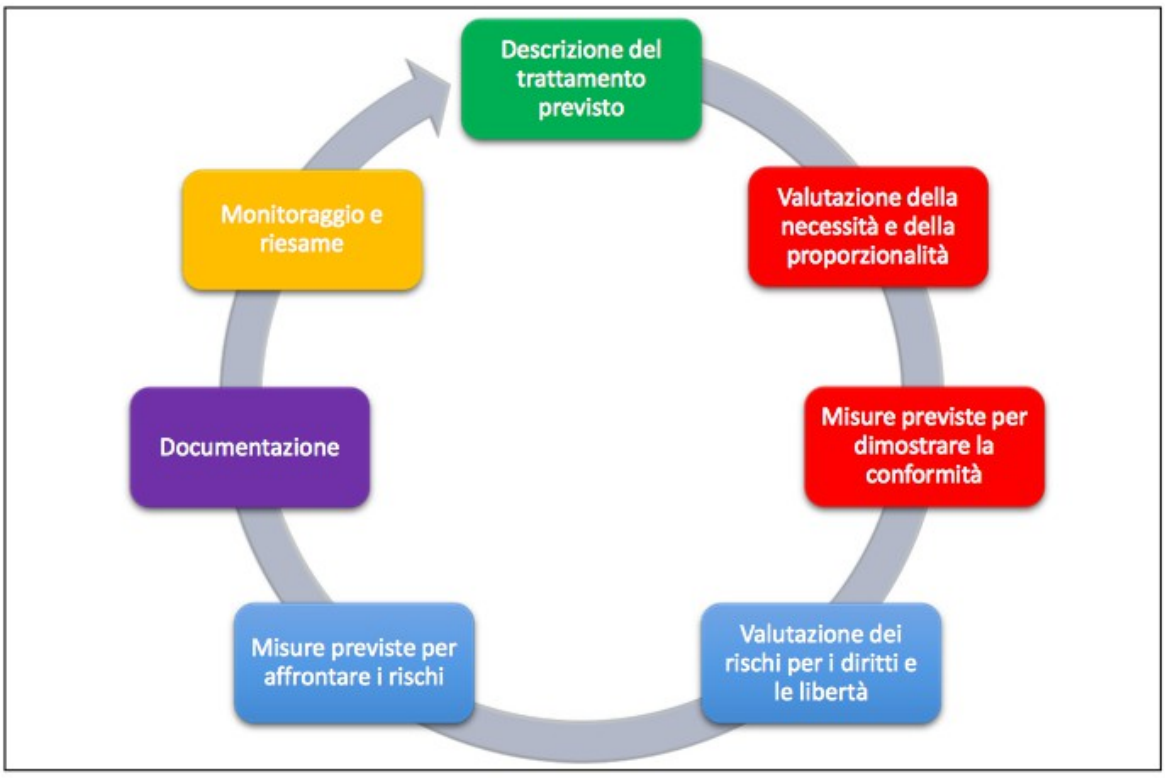
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio di Protezione Civile
SERVIZIO: denominazione e punti di contatto	Servizio di Protezione Civile
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Modica Di Marco Francesco
Incaricati trattamento: denominazione e punti di contatto	sig. Gentini Gian Mario Sig.ra Oblato Lara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 36 - I dati possono essere raccolti sia presso l'interessato, sia presso terzi (ASL, Regione, Provincia, Prefettura, Associazioni di Volontariato di protezione civile, Vigili del Fuoco, Corpo forestale, Autorita' di Pubblica Sicurezza) vengono quindi comunicati ai soggetti coinvolti nelle azioni di intervento, al fine di permettere l'erogazione mirata del servizio. Ai fini della predisposizione della programmazione e dell'adozione dei piani di emergenza in materia di protezione civile, il Comune acquisisce dati inerenti alla dislocazione di strutture e/o abitazioni i cui abitanti, per caratteristiche sanitarie o di disagio psicologico, acquisiscono priorita' in situazioni di emergenza

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 36 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art.

copia informatica per consultazione

	1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D. Lgs. 31 marzo 1998, n. 112, art. 108; Legge 24 febbraio 1992, n. 225, art. 6; Legge 9 novembre 2001, n.401; D.P.R. 8 febbraio 2001 n. 194; Regolamenti comunali in materia
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 36 - Sistema informativo relativo a sicurezza e ordine pubblico - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 36 - Trattamento effettuato per finalita' di protezione civile. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 36 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonche' compiti di igiene e sicurezza sui luoghi di

copia informatica per consultazione

	lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumita' fisica ai sensi dell'art. 2-sexies, comma 2 lett. u) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (svolgimento delle competenze che la legge demanda all'Ente locale in materia di protezione civile)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 36 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) ASL, Aziende ospedaliere e Regioni (per comunicare l'evoluzione della situazione, i controlli e le verifiche periodiche, il monitoraggio dell'attivita'); b) Organi di Polizia / Carabinieri (cui vengono comunicate le attivita' di pubblica sicurezza)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di*	

copia informatica per consultazione

ubicazione del/i server	
Categorie di interessati	- Persone fisiche
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

copia informatica per consultazione

	- MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**

copia informatica per consultazione

art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Servizi di protezione civile

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Economato
SERVIZIO	Servizio Economato

TRATTAMENTO	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

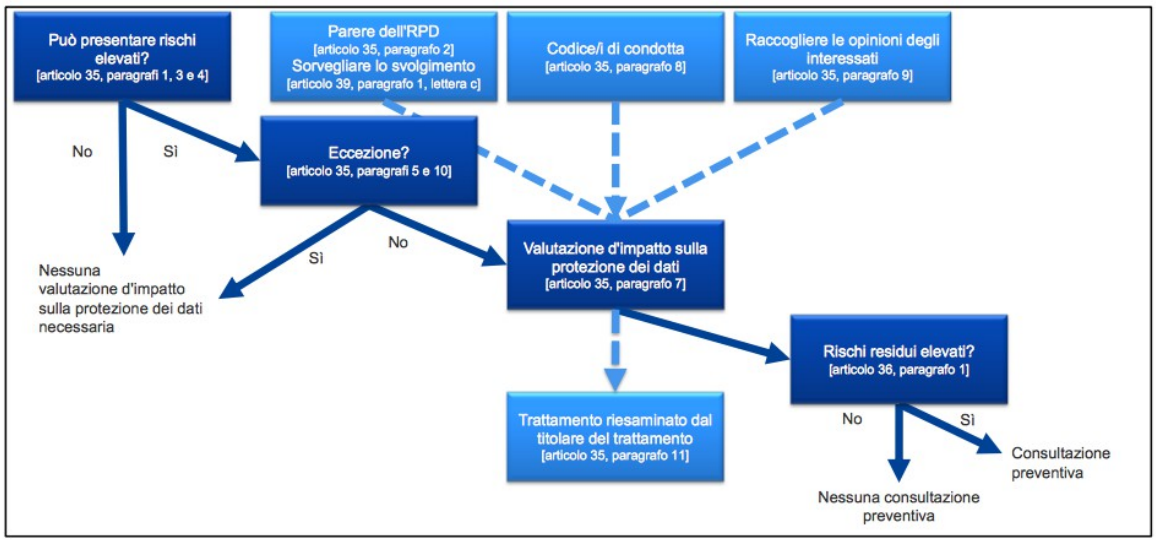
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

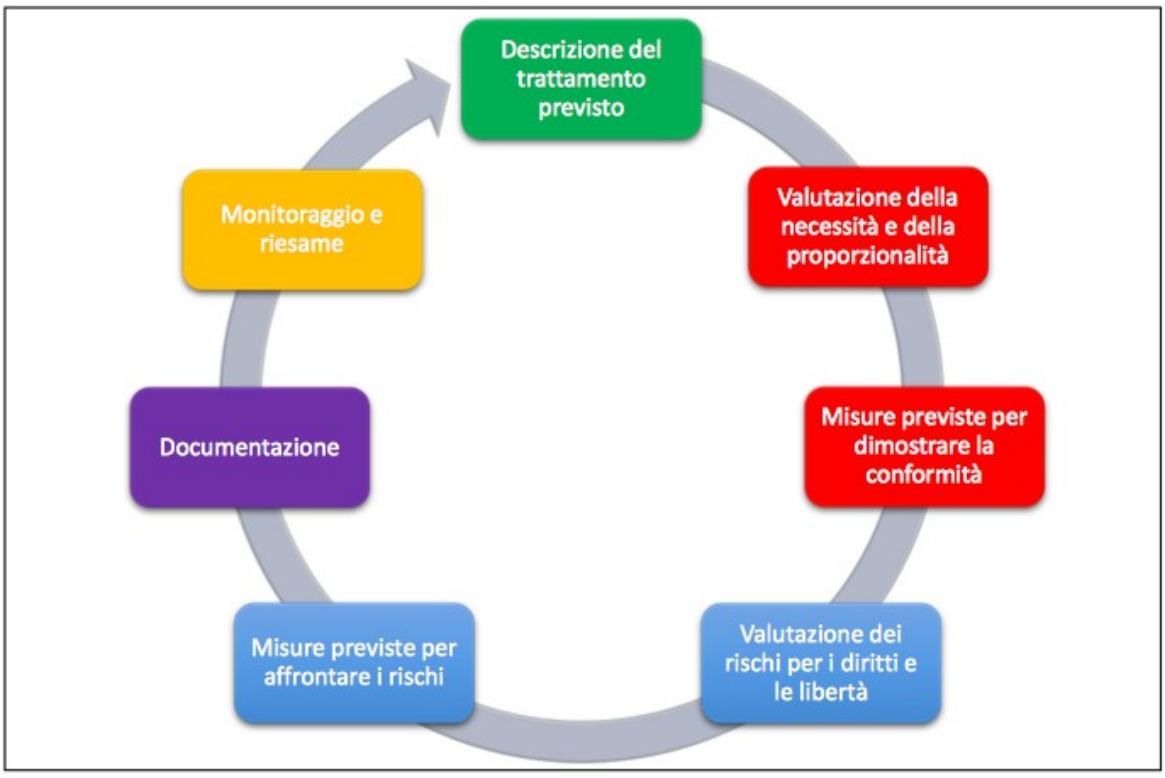
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Economato
SERVIZIO: denominazione e punti di contatto	Servizio Economato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Servidei Stefano
Incaricati trattamento: denominazione e punti di contatto	Sig. Baldetti Giancarlo

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 50 - Il trattamento ha per oggetto i dati delle procedure di affidamento e dei contratti di appalto e di concessione delle amministrazioni aggiudicatrici e degli enti aggiudicatori per l'acquisizione di servizi, forniture, lavori e opere, nonche' i concorsi pubblici di progettazione e l'attivita' posta in essere in attuazione del D.Lgs. n. 50/2016. I dati vengono raccolti dai soggetti partecipanti alle procedure di affidamento e includono dati sensibili e giudiziari. Il trattamento implica, oltre alle ordinarie forme di elaborazione standardizzate (con mezzi elettronici e su supporto cartaceo), anche la comunicazione a terzi e, in particolare, alle Autorita' competenti a rilasciare le certificazioni sul possesso dei requisiti, nonche' la possibile diffusione mediante pubblicazione sul profilo del committente e sui siti web prescritti dalla normativa vigente in materia.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Fonte normativa	- Scheda n. 50 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001- Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 50/2016 - Linee Guida Anac - Statuto - Regolamento sul procedimento amministrativo - Regolamento sull'attivita' contrattuale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza trasversalmente, di tutti gli uffici che aggiudicano contratti inclusi nell'ambito di applicazione del D.Lgs. 50 n. 0/2016
Nome archivio/Banca dati	- Scheda n. 50 - Sistema informativo relativo ad appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili - Dati relativi al comportamento debitorio - Dati relativi all'affidabilita' o puntualita' nei pagamenti - Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati relativi all'adempimento di obbligazioni - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti - Dati relativi all'affidabilita' nell'esecuzione dei contratti pubblici
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del	- Scheda n. 50 - Trattamento effettuato per finalita' di adempimento di obblighi

copia informatica per consultazione

trattamento	contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 50 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 50 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Agenzia Entrate, Prefettura, Tribunale, Procura presso il Tribunale, Provincia e altri enti pubblici - INPS/INAIL/ANAC - , anche attraverso la consultazione delle relative Banche dati, per i controlli sul possesso dei requisiti dichiarati in sede di procedura di affidamento; b) altri soggetti partecipanti alla procedura di affidamento; c) consulenti e soggetti, pubblici o privati, che effettuano servizi di committenza ausiliaria; d) avvocati incaricati dell'eventuale contenzioso (ai sensi del D.Lgs. n. 50/2016 e della regolazione attuativa)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione sul sito web, in "Amministratrazione trasparente" in attuazione di obblighi di pubblicazione di cui al D. Lgs. n. 33/2013 - Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base

copia informatica per consultazione

	normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: ***trasferimento all'estero***	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Concorrenti alle procedure di affidamento di contratti pubblici - Soggetti terzi rispetto ai concorrenti, i cui dati rilevano nella procedura di affidamento
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD

copia informatica per consultazione

(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli

copia informatica per consultazione

	atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento

copia informatica per consultazione

rischi: ***accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale

copia informatica per consultazione

	Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON

copia informatica per consultazione

	AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare

copia informatica per consultazione

- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

- La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

-

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale	

copia informatica per consultazione

	Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti

copia informatica per consultazione

	- MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4

copia informatica per consultazione

Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Consegna arredi e attrezzature uffici
Fornitura cancelleria ed altro materiale di consumo per gli uffici

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Servizio Lavori pubblici
SERVIZIO	Servizio Lavori Pubblici

TRATTAMENTO	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

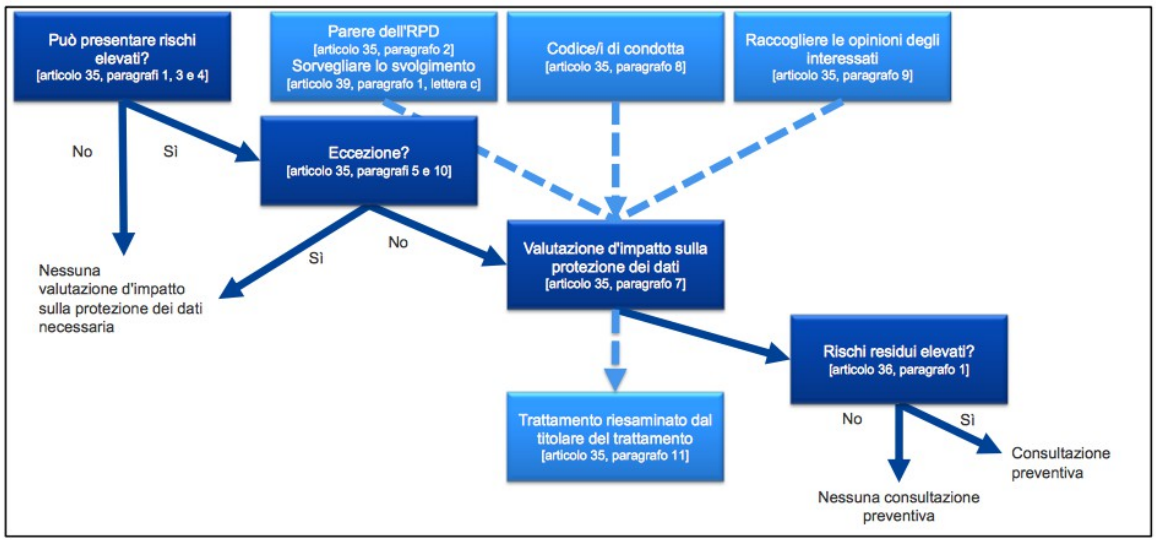
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

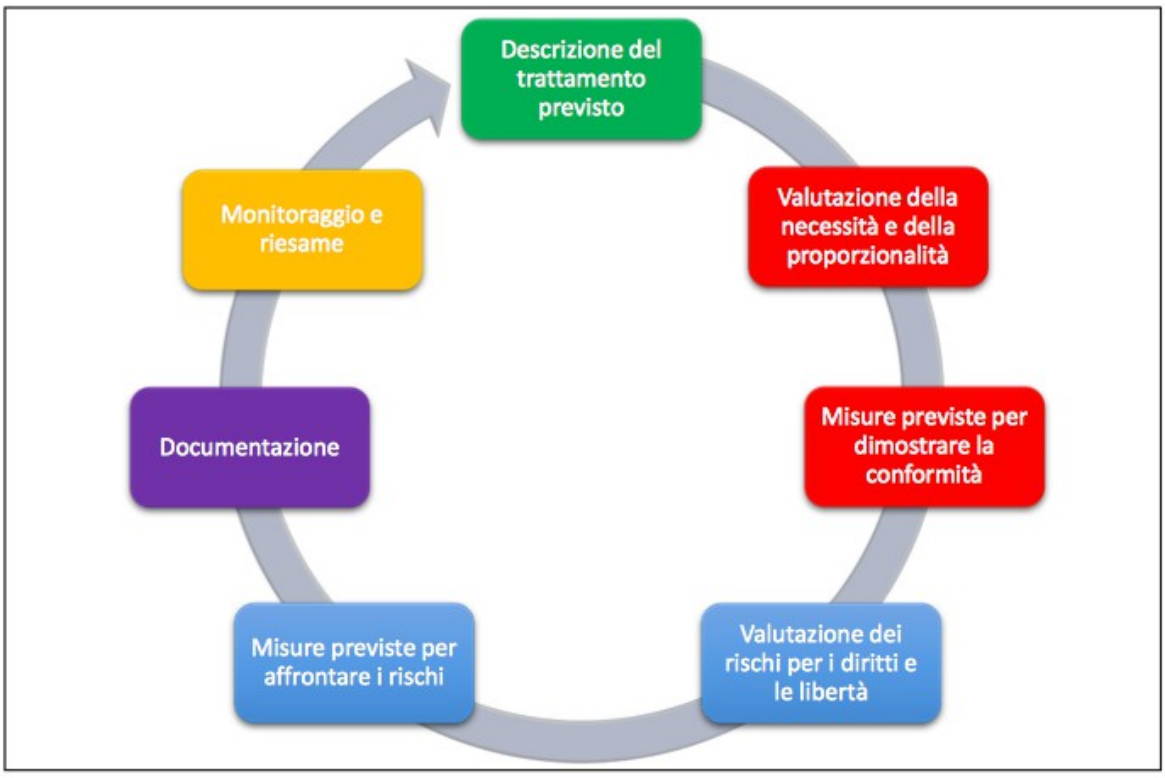
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	05 - Area tecnica Lavori Pubblici e Ambiente
SERVIZIO	Servizio Lavori pubblici
SERVIZIO: denominazione e punti di contatto	Servizio Lavori Pubblici
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Arch. Braccesi Priscilla
Incaricati trattamento: denominazione e punti di contatto	sig. Cavicchioli Gaetano sig. Corsi Francesco sig. Piacentini Simone Dott. Dini Carlo

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 50 - Il trattamento ha per oggetto i dati delle procedure di affidamento e dei contratti di appalto e di concessione delle amministrazioni aggiudicatrici e degli enti aggiudicatori per l'acquisizione di servizi, forniture, lavori e opere, nonche' i concorsi pubblici di progettazione e l'attivita' posta in essere in attuazione del D.Lgs. n. 50/2016. I dati vengono raccolti dai soggetti partecipanti alle procedure di affidamento e includono dati sensibili e giudiziari. Il trattamento implica, oltre alle ordinarie forme di elaborazione standardizzate (con mezzi elettronici e su supporto cartaceo), anche la comunicazione a terzi e, in particolare, alle Autorita' competenti a rilasciare le certificazioni sul possesso dei requisiti, nonche' la possibile diffusione mediante pubblicazione sul profilo del committente e sui siti web prescritti dalla normativa vigente in materia.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 50 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001- Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 50/2016 - Linee Guida Anac - Statuto - Regolamento sul procedimento amministrativo - Regolamento sull'attivita' contrattuale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza trasversalmente, di tutti gli uffici che aggiudicano contratti inclusi nell'ambito di applicazione del D.Lgs. 50 n. 0/2016
Nome archivio/Banca dati	- Scheda n. 50 - Sistema informativo relativo ad appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili - Dati relativi al comportamento debitorio - Dati relativi all'affidabilita' o puntualita' nei pagamenti - Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati relativi all'adempimento di obbligazioni - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti - Dati relativi all'affidabilita' nell'esecuzione dei contratti pubblici
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi

copia informatica per consultazione

Finalita' del trattamento	- Scheda n. 50 - Trattamento effettuato per finalita' di adempimento di obblighi contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 50 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 50 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Agenzia Entrate, Prefettura, Tribunale, Procura presso il Tribunale, Provincia e altri enti pubblici - INPS/INAIL/ANAC - , anche attraverso la consultazione delle relative Banche dati, per i controlli sul possesso dei requisiti dichiarati in sede di procedura di affidamento; b) altri soggetti partecipanti alla procedura di affidamento; c) consulenti e soggetti, pubblici o privati, che effettuano servizi di committenza ausiliaria; d) avvocati incaricati dell'eventuale contenzioso (ai sensi del D.Lgs. n. 50/2016 e della regolazione attuativa)
Categorie di trattamenti - particolari forme di elaborazione:	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione sul sito web, in "Amministratrazione trasparente" in attuazione di obblighi di pubblicazione di cui al D. Lgs. n. 33/2013

copia informatica per consultazione

diffusione	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Concorrenti alle procedure di affidamento di contratti pubblici - Soggetti terzi rispetto ai concorrenti, i cui dati rilevano nella procedura di affidamento
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

cartacei o canali di trasmissione	
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II

copia informatica per consultazione

VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la

copia informatica per consultazione

	consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

RISCHI **Origine/fonte dei rischi:** ***accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle

copia informatica per consultazione

	password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC

copia informatica per consultazione

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

copia informatica per consultazione

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative	

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi

copia informatica per consultazione

	- MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

copia informatica per consultazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Programmazione dei lavori art. 21
Programmazione di forniture e di servizi

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO NOTIFICA
SERVIZIO	Servizio Notifica

TRATTAMENTO	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

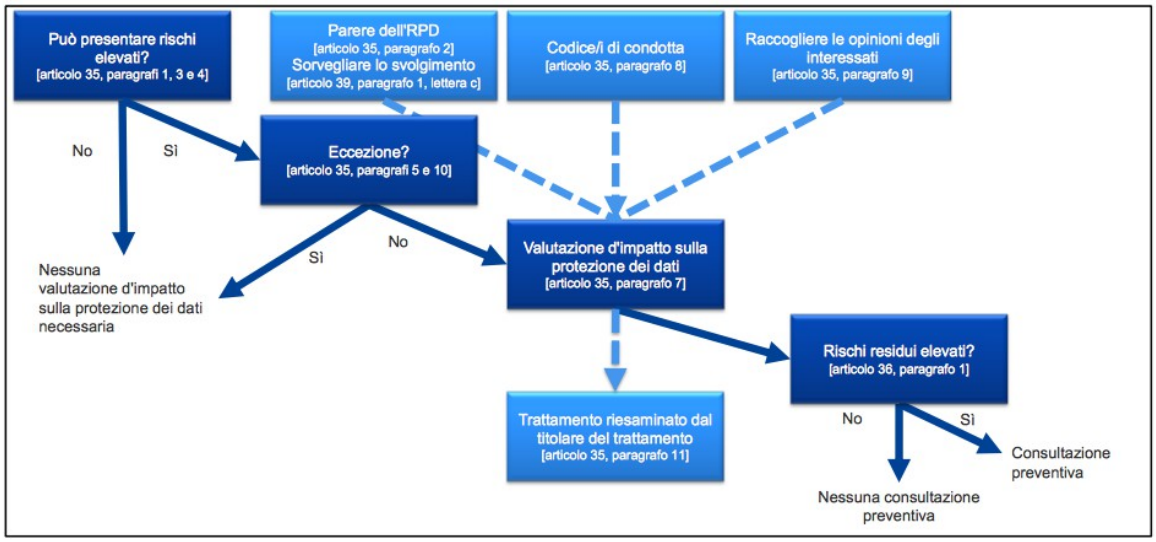
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

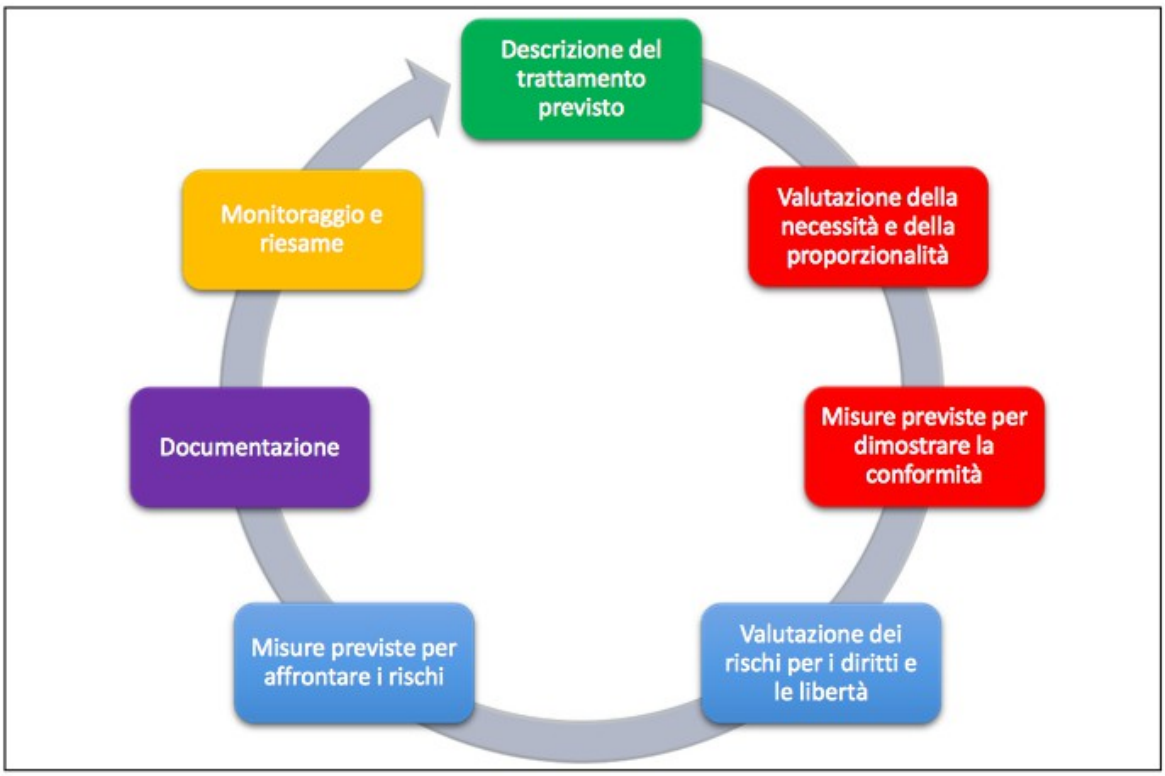
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO NOTIFICA
SERVIZIO: denominazione e punti di contatto	Servizio Notifica
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Danesi Sauro

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 57 - I dati vengono raccolti sia presso l'ente, sia presso terzi, sia presso gli interessati. Si pensi in particolare, sotto tale profilo, alla tenuta degli Albi, che comporta talvolta l'acquisizione ed il trattamento anche di dati vulnerabili e sensibili. Il trattamento avviene per rilevanti finalita' di interesse pubblico relative verifica della legittimita' dell'iscrizione negli albi o a modifiche rispetto all'iscrizione, con riferimento in particolare, al buon andamento, all'imparzialita' dell'attivita' amministrativa, nonche' alla rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti (art. 67, co.1, lett.a) d.Lgs. 196/2003). Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo tramite sistema informativo di notifiche e deposito atti amministrativi e giudiziari , comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n.114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 57 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice di procedura civile
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 57 - Sistema informativo relativo al sistema informativo notifiche e deposito atti amministrativi e giudiziari - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 57 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: segreteria generale. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 57 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: volgimento delle funzioni di controllo, indirizzo politico,inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di

copia informatica per consultazione

	razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 57 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) soggetti privati e pubblici (D.Lgs. 267/2000 - Codice di procedura civile)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	

copia informatica per consultazione

Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto

copia informatica per consultazione

Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Albo e notifiche: Notifiche
Albo e inviti: Inviti consigli comunali
Albo: Pubblicazioni albo on-line

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio Polizia amministrativa
SERVIZIO	Servizio Polizia Ammistrativa

TRATTAMENTO	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

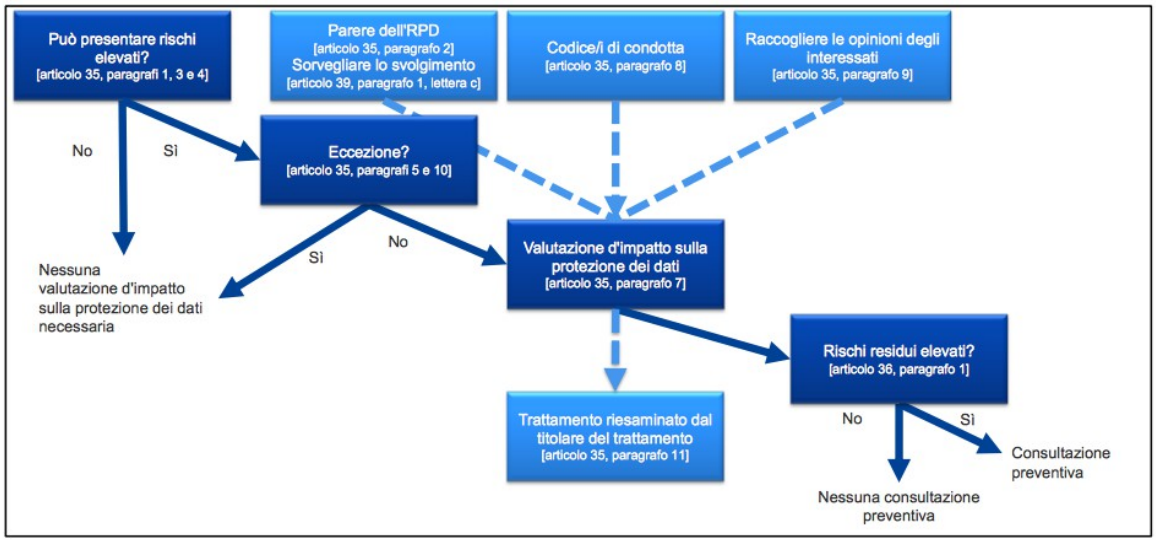
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

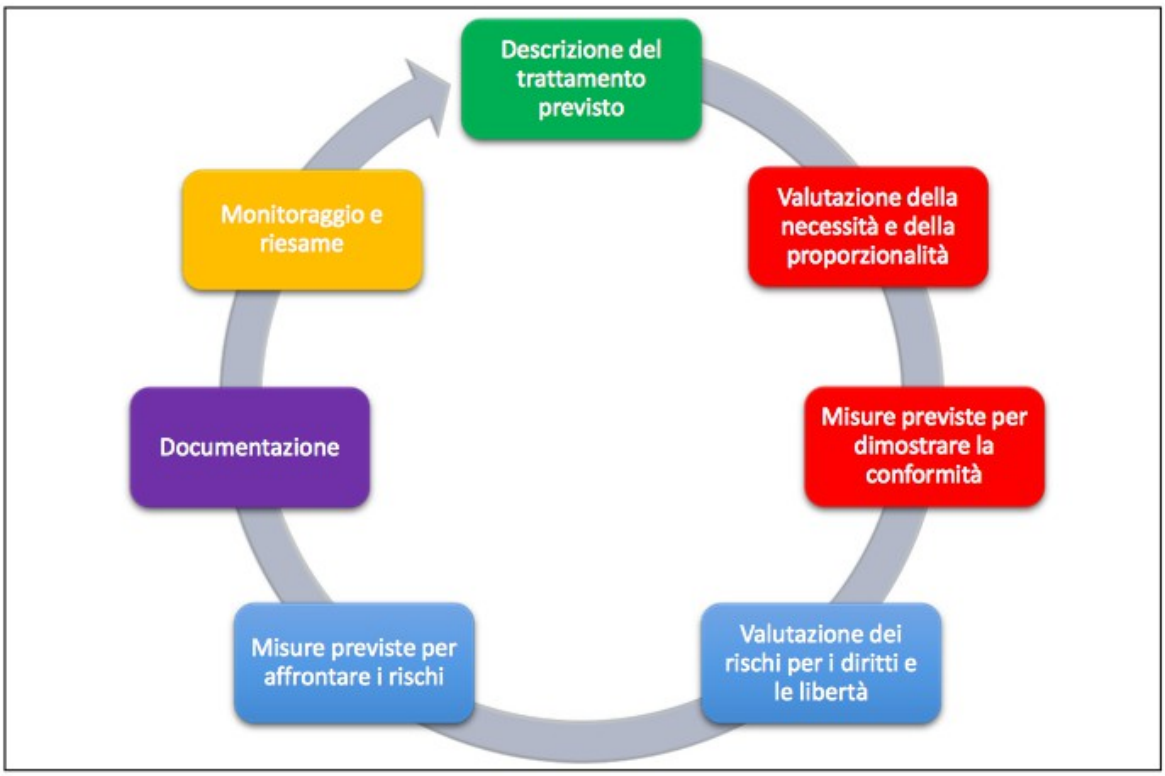
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio Polizia amministrativa
SERVIZIO: denominazione e punti di contatto	Servizio Polizia Ammistrativa
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Modica Di Marco Francesco
Incaricati trattamento: denominazione e punti di contatto	sig.ra Lupi Claudia sig. Orzati Massimiliano sig. Cottone Pietro Sig.ra Oblato Lara Sig.ra Martorella Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 25 - I dati vengono acquisiti tramite i verbali elevati da enti e Forze dell'ordine e/o ispezioni effettuate dagli organi addetti al controllo; tuttavia essi possono essere reperiti anche direttamente dagli interessati, qualora gli stessi presentino dei ricorsi.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 25 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n.

copia informatica per consultazione

	267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 24.11.1981, n. 689 - D.Lgs. 30.04.1992, n. 285 (art. 116) - D.P.R. 16.12.1992, n. 495 - D.Lgs. 18.08.2000, n. 267
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 25 - Sistema informativo relativo alla gestione delle procedure sanzionatorie - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 25 - Trattamento effettuato per finalita' di rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 25 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' sanzionatorie e di tutela in sede amministrativa o giudiziaria ai sensi dell'art. 2-sexies, comma 2, lett. q), D.Lgs. n. 196/2003 come

copia informatica per consultazione

	modificato dal D.Lgs. n. 101/2018 (applicazione delle norme in materia di sanzioni amministrative e ricorsi)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 25 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Dipartimento per i trasporti terrestri e Prefettura (art. 223, d.lgs. n. 285/1992)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di	- Utenti (anche potenziali)

copia informatica per consultazione

interessati	
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli

copia informatica per consultazione

interessati o loro rappresentanti	interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative

copia informatica per consultazione

	al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Controlli sull'abbandono di rifiuti urbani

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio Polizia amministrativa
SERVIZIO	Servizio Polizia Ammistrativa

TRATTAMENTO	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

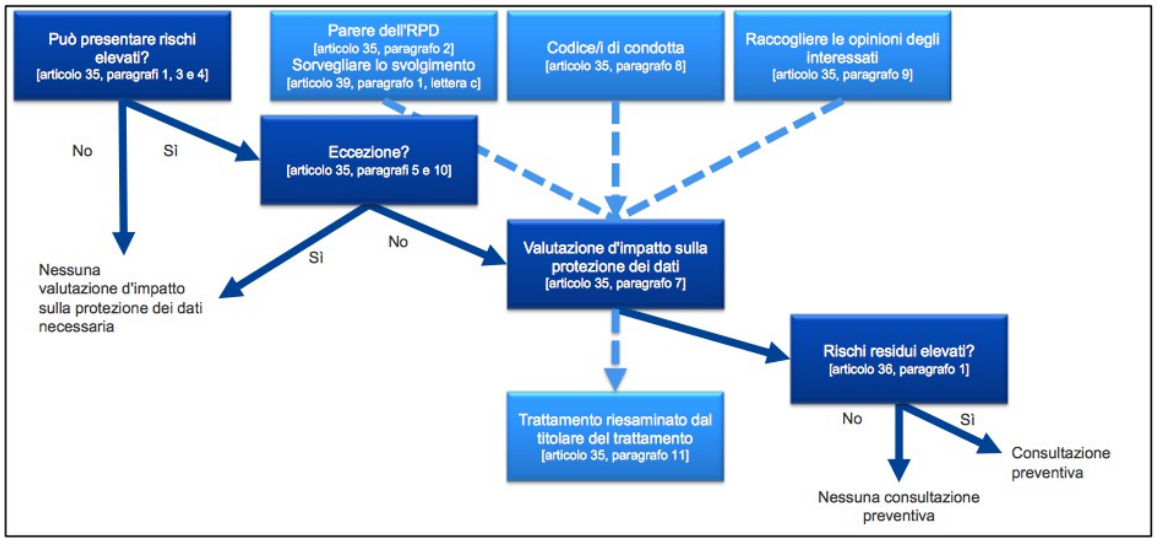
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

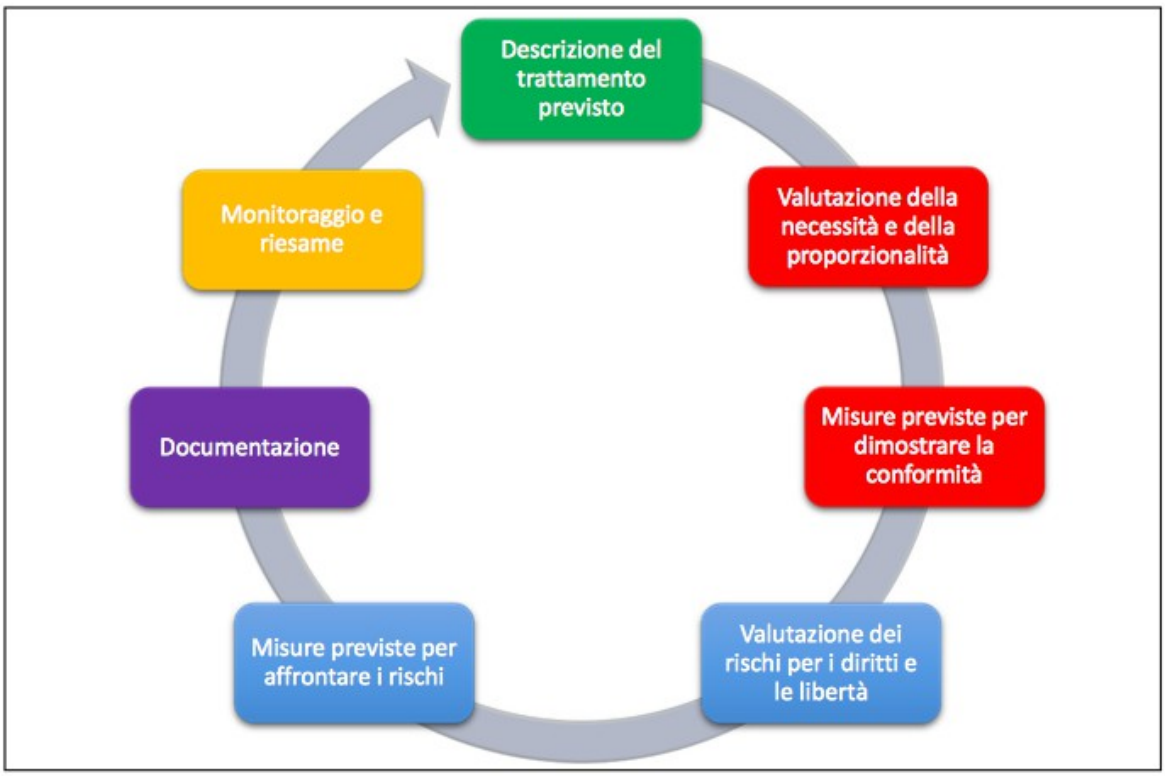
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio Polizia amministrativa
SERVIZIO: denominazione e punti di contatto	Servizio Polizia Ammistrativa
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Modica Di Marco Francesco
Incaricati trattamento: denominazione e punti di contatto	sig.ra Lupi Claudia sig. Orzati Massimiliano sig. Cottone Pietro Sig.ra Oblato Lara Sig.ra Martorella Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 26 - I dati (in particolare quelli contenuti nel c.d. "certificato antimafia") vengono acquisiti dagli interessati al momento della presentazione delle domande per le licenze o per le autorizzazioni amministrative; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti. I dati sulla salute vengono trattati, in particolare, al fine di verificare i requisiti richiesti nel caso di soggetti preposti alla gestione di determinate attivita', come ad esempio la rivendita di generi alimentari. I dati possono essere anche acquisiti attraverso i controlli svolti presso l'esercizio o l'attivita' dell'interessato, al fine di verificare le autorizzazioni e la relativa regolarita'; in tal caso viene redatto un verbale di ispezione, cui segue una verifica presso gli uffici comunali competenti.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 26 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo R.d. 18.06.1931, n. 773 (artt. 5 e 75) - L. 28.03.1991, n. 112 - D.Lgs. 31.03.1998, n. 114 - D.P.R. 30.4.1999, n. 162 - D.P.R. 26.10.2001, n. 430 - D.P.R. 24.07.1977, n. 616 (art. 19) - regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 26 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 26 - Trattamento effettuato per finalita' di ordine e sicurezza pubblica. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 26 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di polizia amministrativa locale, con particolare riferimento ai servizi di igiene)

copia informatica per consultazione

Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Altre amministrazioni ed enti pubblici - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.

copia informatica per consultazione

Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione

copia informatica per consultazione

Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative

copia informatica per consultazione

	al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Controlli sull'uso del territorio
Vigilanza e verifiche su mercati ed ambulanti

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio Polizia amministrativa
SERVIZIO	Servizio Polizia Ammistrativa

TRATTAMENTO	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

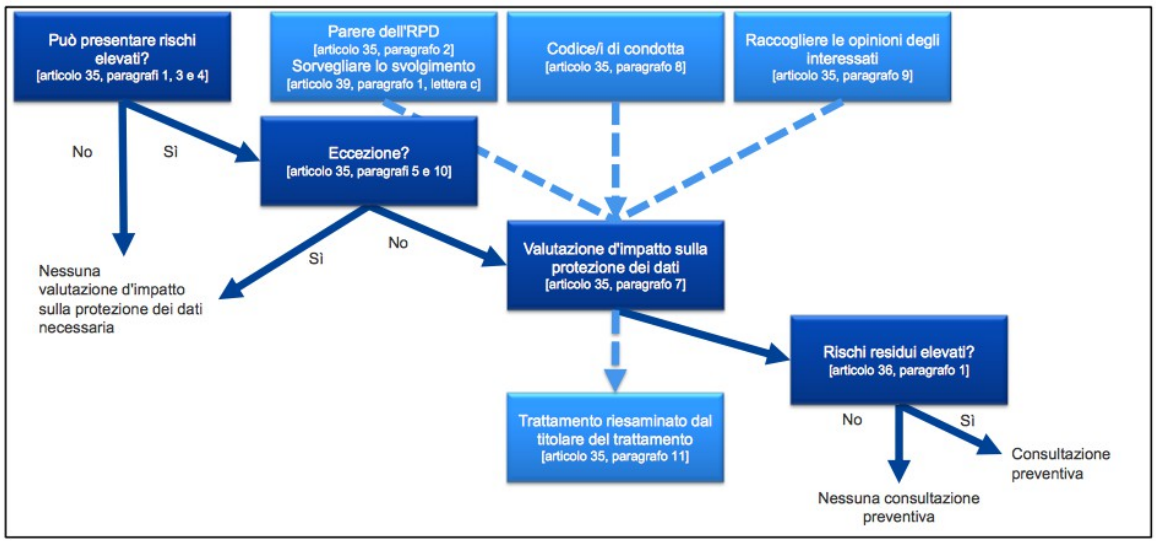
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

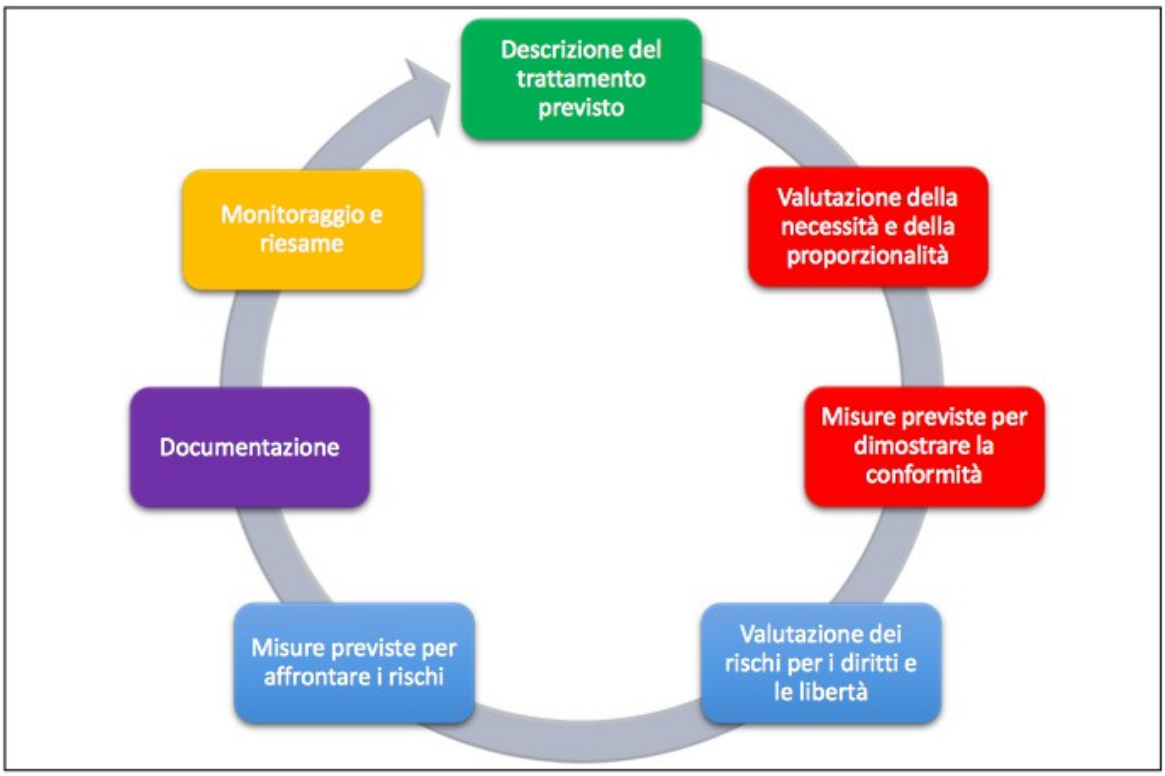
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio Polizia amministrativa
SERVIZIO: denominazione e punti di contatto	Servizio Polizia Ammistrativa
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Modica Di Marco Francesco
Incaricati trattamento: denominazione e punti di contatto	sig.ra Lupi Claudia sig. Orzati Massimiliano sig. Cottone Pietro Sig.ra Oblato Lara Sig.ra Martorella Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 42 - I dati vengono acquisiti dagli interessati al momento del sopralluogo e dell'ispezione o verifica; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti o eventuali violazioni rispetto alle dichiarazioni acquisite. I dati sono registrati in archivi/ banche di dati gestite con modalita' elettroniche e su supporti cartacei tramite sistema informativo, controlli esterni, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 42 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni

copia informatica per consultazione

	(LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - D.Lg. n. 50/2016 - Reg. UE 679/2016 - DL. 24 novembre 1981 n. 689 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sui controlli interni
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 42 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 42 - Trattamento effettuato per attivita' di controllo, ispettive, comprese le attivita' di sopralluogo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 42 -Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di controllo, ispettive, comprese le attivita' di sopralluogo con la polizia locale)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una

copia informatica per consultazione

	delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 42 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Autorita' giudiziaria, autorita' di pubblica sicurezza (per accertamenti di carattere giudiziario); b) al RUP e alla stazione appaltante (D.Lgs. n. 50/2016); c) alle autorita' amministrative di vigilanza (D.Lgs. n. 50/2016)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Persone fisiche - Cittadini italiani - Persone giuridiche ed altri enti (comprende societa' di persone) - Cittadini di Paesi appartenenti all'U.E.

copia informatica per consultazione

	- Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione

copia informatica per consultazione

rappresentanti	
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative

copia informatica per consultazione

	al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Accertamenti e controlli sull'attivita' edilizia privata (abusi)

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio polizia urbana
SERVIZIO	Servizio Polizia Urbana

TRATTAMENTO	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

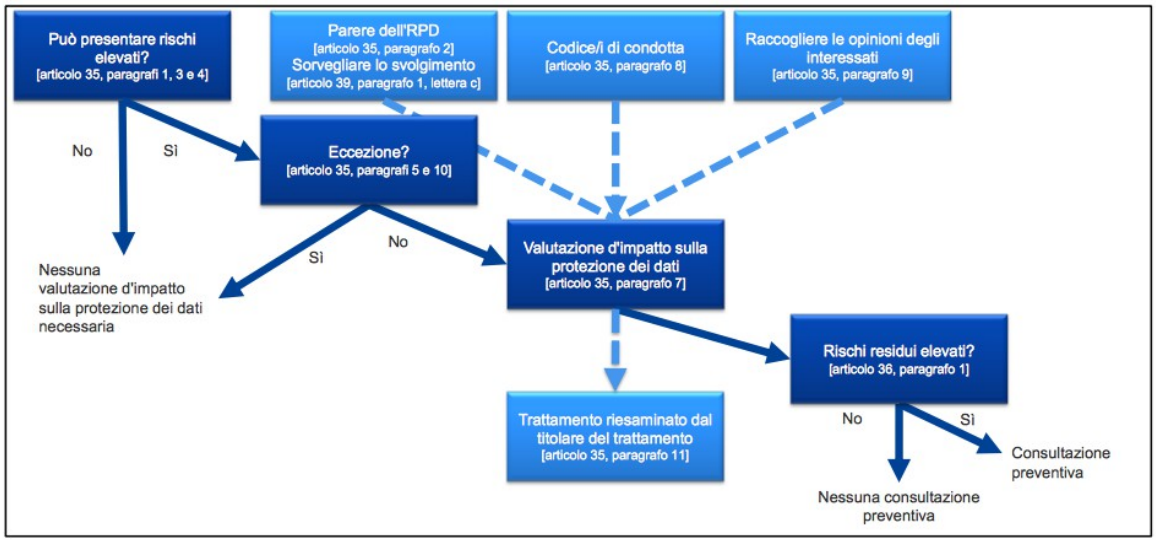
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

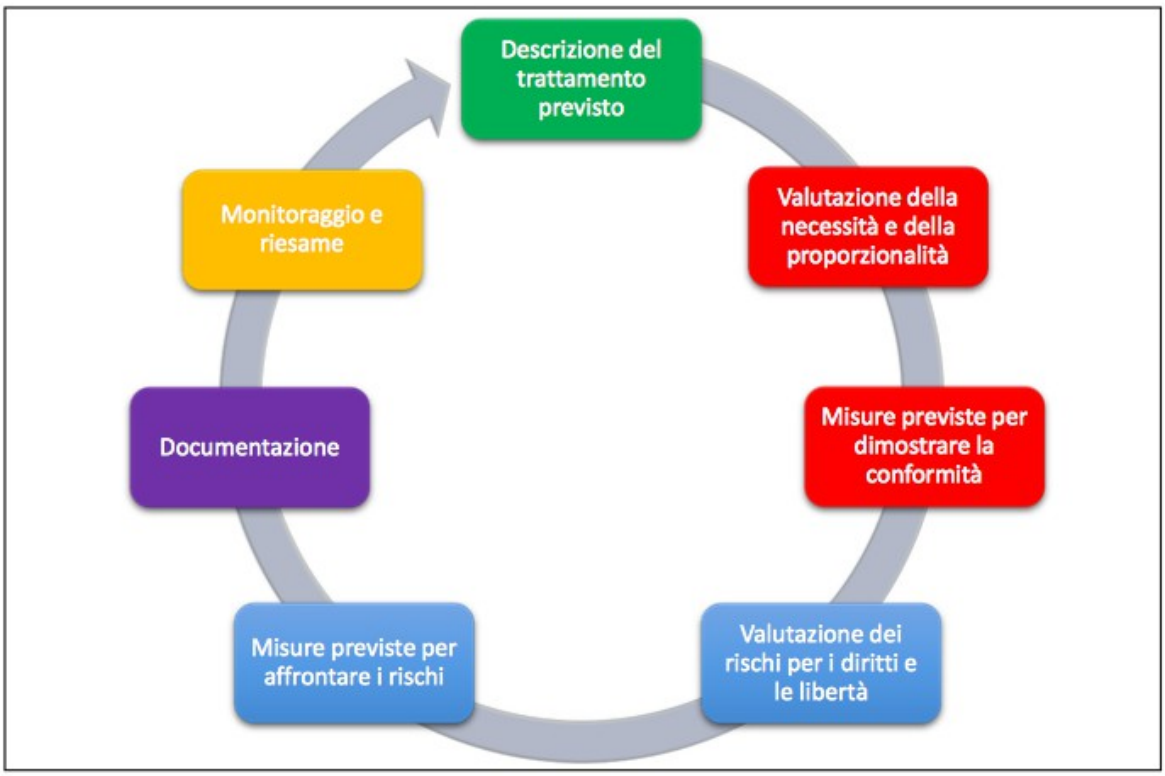
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio polizia urbana
SERVIZIO: denominazione e punti di contatto	Servizio Polizia Urbana
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Modica Di Marco Francesco
Incaricati trattamento: denominazione e punti di contatto	sig.ra Giovani Luciana sig.ra Lupi Claudia sig. Munno Cesare Sig.ra Oblato Lara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 25 - I dati vengono acquisiti tramite i verbali elevati da enti e Forze dell'ordine e/o ispezioni effettuate dagli organi addetti al controllo; tuttavia essi possono essere reperiti anche direttamente dagli interessati, qualora gli stessi presentino dei ricorsi.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 25 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n.

copia informatica per consultazione

	196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 24.11.1981, n. 689 - D.Lgs. 30.04.1992, n. 285 (art. 116) - D.P.R. 16.12.1992, n. 495 - D.Lgs. 18.08.2000, n. 267
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 25 - Sistema informativo relativo alla gestione delle procedure sanzionatorie - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 25 - Trattamento effettuato per finalita' di rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 25 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' sanzionatorie e di tutela in sede amministrativa o giudiziaria ai sensi dell'art. 2-sexies, comma 2, lett. q), D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (applicazione delle norme in materia di sanzioni

copia informatica per consultazione

	amministrative e ricorsi)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 25 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Dipartimento per i trasporti terrestri e Prefettura (art. 223, d.lgs. n. 285/1992)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Utenti (anche potenziali)

copia informatica per consultazione

Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione

copia informatica per consultazione

Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative

copia informatica per consultazione

	al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Gestione delle sanzioni per violazione del Codice della strada

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio polizia urbana
SERVIZIO	Servizio Polizia Urbana

TRATTAMENTO	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

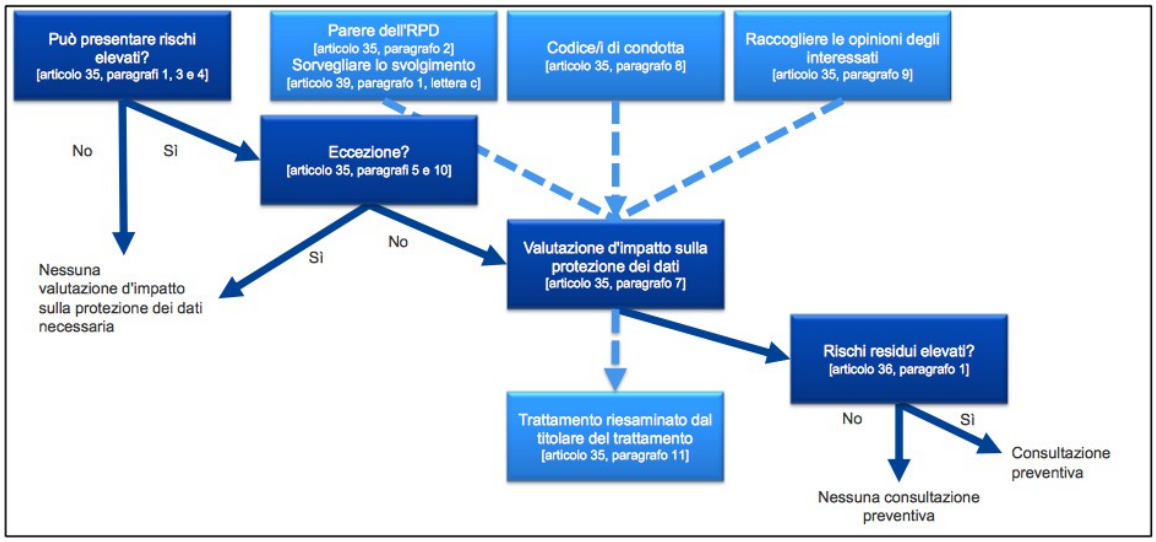
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

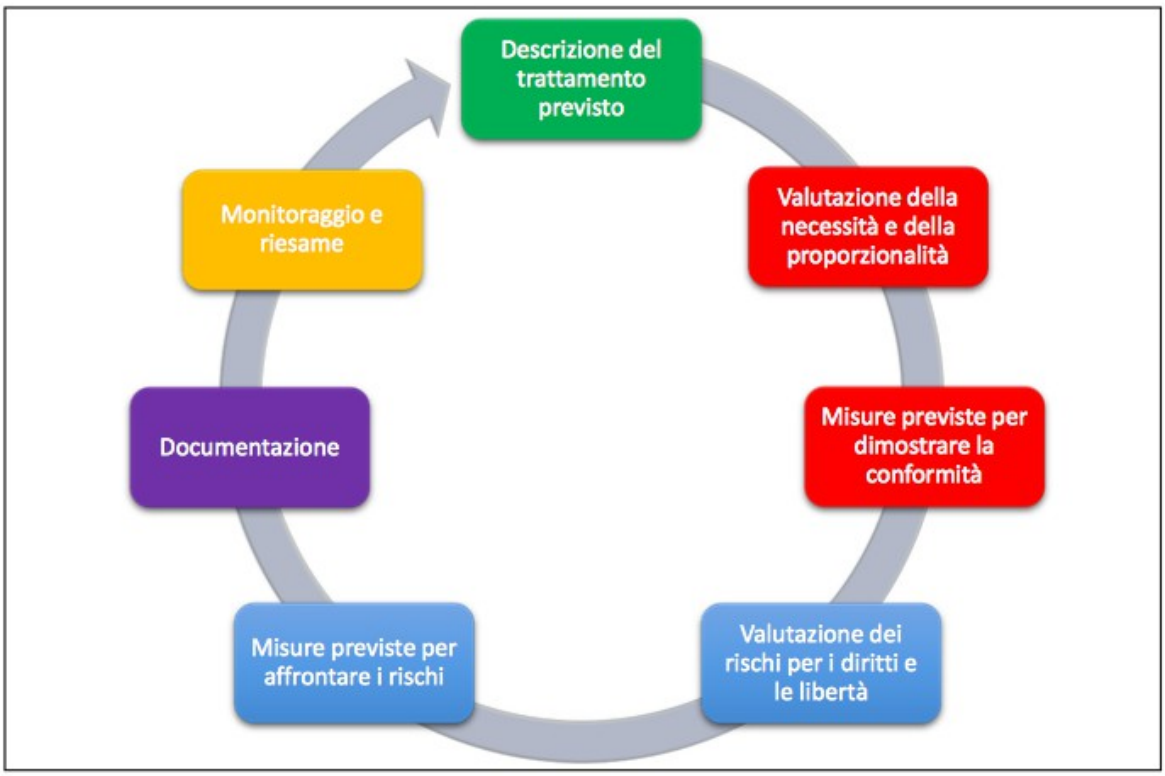
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio polizia urbana
SERVIZIO: denominazione e punti di contatto	Servizio Polizia Urbana
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Fabio Pierulivo Impianti Elettrici e televisivi Abaco SpA STS srl Maggioli Informatica SpA
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Modica Di Marco Francesco
Incaricati trattamento: denominazione e punti di contatto	sig.ra Giovani Luciana sig.ra Lupi Claudia sig. Munno Cesare Sig.ra Oblato Lara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 26 - I dati (in particolare quelli contenuti nel c.d. "certificato antimafia") vengono acquisiti dagli interessati al momento della presentazione delle domande per le licenze o per le autorizzazioni amministrative; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti. I dati sulla salute vengono trattati, in particolare, al fine di verificare i requisiti richiesti nel caso di soggetti preposti alla gestione di determinate attivita', come ad esempio la rivendita di generi alimentari. I dati possono essere anche acquisiti attraverso i controlli svolti presso l'esercizio o l'attivita' dell'interessato, al fine di verificare le autorizzazioni e la relativa regolarita'; in tal caso viene redatto un verbale di ispezione, cui segue una verifica presso gli uffici comunali competenti.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 26 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo R.d. 18.06.1931, n. 773 (artt. 5 e 75) - L. 28.03.1991, n. 112 - D.Lgs. 31.03.1998, n. 114 - D.P.R. 30.4.1999, n. 162 - D.P.R. 26.10.2001, n. 430 - D.P.R. 24.07.1977, n. 616 (art. 19) - regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 26 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 26 - Trattamento effettuato per finalita' di ordine e sicurezza pubblica. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 26 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di polizia amministrativa locale, con particolare riferimento ai servizi di igiene)

copia informatica per consultazione

Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Altre amministrazioni ed enti pubblici - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.

copia informatica per consultazione

Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione

copia informatica per consultazione

Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative

copia informatica per consultazione

	al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Vigilanza e verifiche sulle attivita' commerciali in sede fissa

21

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio polizia urbana
SERVIZIO	Servizio Polizia Urbana

TRATTAMENTO	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	00/00/0000

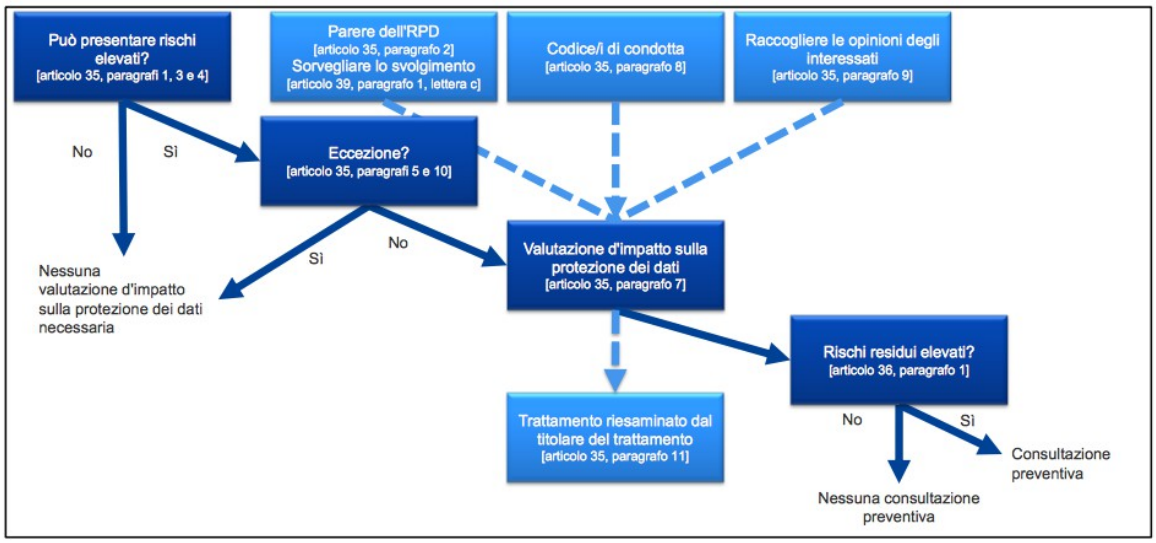
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

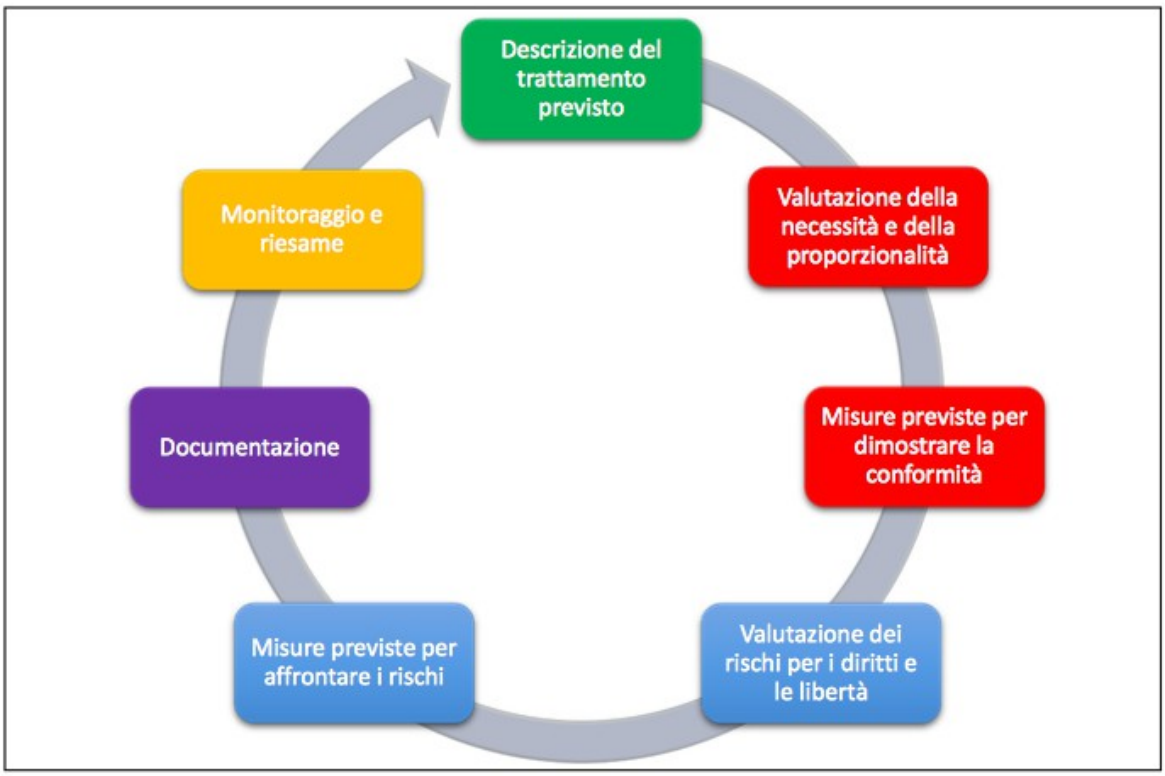
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	06 - Area di Vigilanza
SERVIZIO	Servizio polizia urbana
SERVIZIO: denominazione e punti di contatto	Servizio Polizia Urbana
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Modica Di Marco Francesco
Incaricati trattamento: denominazione e punti di contatto	sig.ra Giovani Luciana sig.ra Lupi Claudia sig. Munno Cesare Sig.ra Oblato Lara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 27 - I dati giudiziari e sulla salute vengono acquisiti attraverso i controlli svolti sul territorio, che sono effettuati su iniziativa d'ufficio, ovvero su richiesta di privati, di enti e di associazioni; oltre alla verifica in loco, vengono avviati i necessari accertamenti presso gli uffici competenti, al termine dei quali viene predisposta una relazione finale con l'indicazione delle eventuali violazioni in materia sanitaria o ambientale riscontrate. In tal caso, si procede a trasmetterle alle competenti autorita' amministrative o penali. Vengono, inoltre, effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000. Per quanto concerne l'attivita' di polizia mortuaria, ed i connessi servizi cimiteriali, i dati vengono forniti direttamente dagli interessati, dai familiari o dal rappresentante della comunita' religiosa, che presentano apposita domanda al Comune al fine di ottenere delle particolari forme di sepoltura. I dati sulla salute vengono trattati in quanto i medici debbono denunciare al sindaco la malattia che, a loro giudizio, sarebbe stata la causa di morte di persona da loro assistita. Il comune a sua volta comunica le cause di morte all'ISTAT per le rilevazioni annuali, nonche' alla ASL competente per territorio per l'aggiornamento del registro delle cause di morte.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 27 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 28.02.1985, n. 47 - D.Lgs. 5.02.1997, n. 22 - D.Lgs. 29.10.1999, n. 490 - D.P.R. 10.09.1990, n. 285 - regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 27 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare lo stato di salute: patologie attuali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 27 - Trattamento effettuato per finalita' relative a: attivita' di polizia amministrativa locale, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente compreso l'inquinamento acustico, tutela delle risorse idriche e difesa del suolo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare

copia informatica per consultazione

Rilevanti finalita' di interesse pubblico	- Scheda n. 27 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di polizia amministrativa locale, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente compreso l'inquinamento acustico, tutela delle risorse idriche e difesa del suolo)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 27 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) ISTAT (per le rilevazioni annuali della cause di morte); b) ASL (per l'aggiornamento del registro delle cause di morte); c) all'ente gestore degli alloggi mortuari (per l'erogazione del servizio)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Persone fisiche - Cittadini italiani - Persone giuridiche ed altri enti (comprende societa' di persone)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Organismi del servizio sanitario nazionale - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati

copia informatica per consultazione

	esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento

copia informatica per consultazione

finalita'	quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza

copia informatica per consultazione

	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli	Alto

copia informatica per consultazione

interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

copia informatica per consultazione

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza:	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica	

copia informatica per consultazione

tecniche logistiche	- MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non

copia informatica per consultazione

	autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione Responsabile di Posizione Organizzativa individuato in base agli atti di organizzazione, competente per materia a gestire l'attivita' e il trattamento dei dati

copia informatica per consultazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Sicurezza ed ordine pubblico
Vigilanza sulla circolazione e la sosta

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO	Servizio Scuola e Biblioteca

TRATTAMENTO	Scheda n. 11 - Servizi sociali - Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

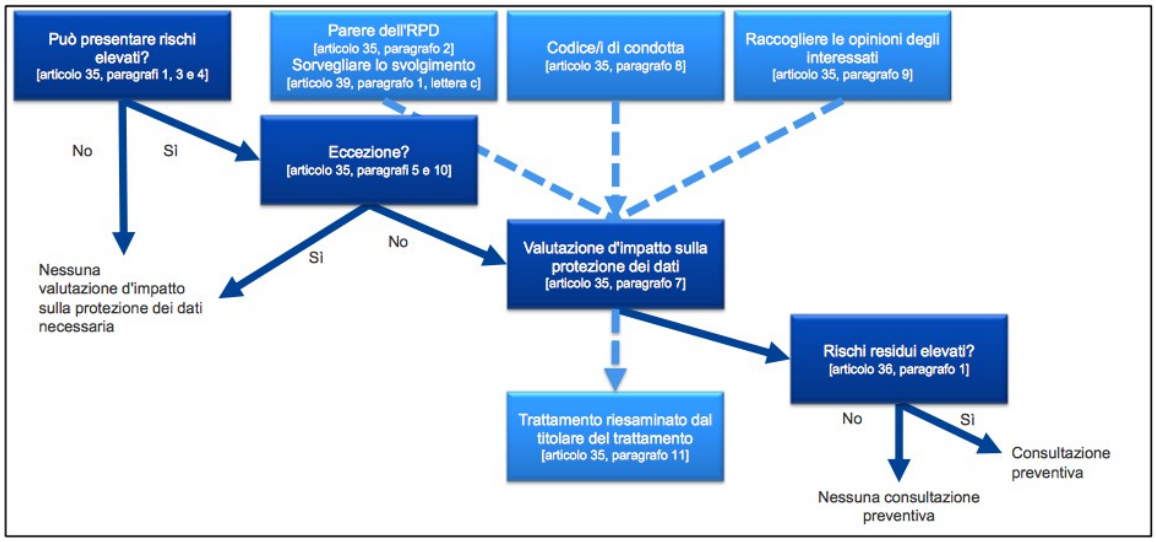
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

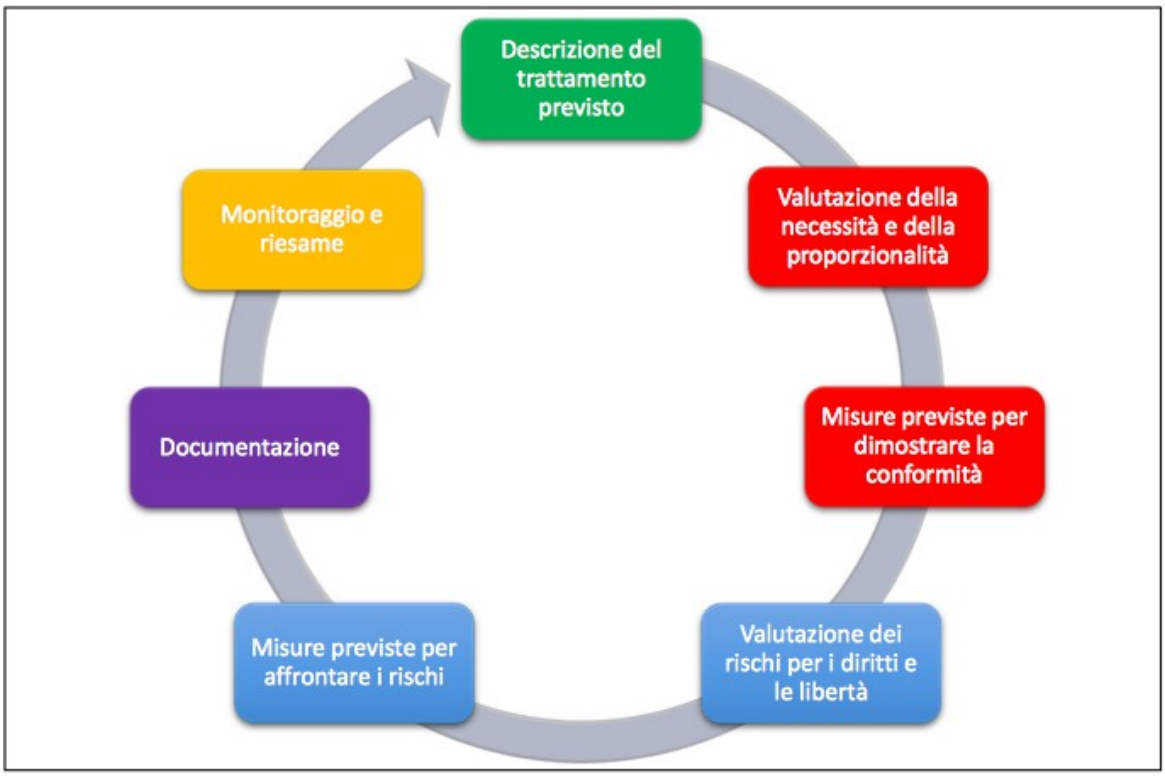
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO: denominazione e punti di contatto	Servizio Scuola e Biblioteca
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 11- I dati vengono forniti dall'interessato o da terzi (ASL, Scuole dell'infanzia e Istituti di istruzione). Le informazioni necessarie sono comunicate agli enti convenzionati che effettuano l'intervento ed agli istituti scolastici, nonche' alle regioni a fini di rendicontazione e monitoraggio dell'attivita'; sono, inoltre, comunicati alla ASL competente per il riconoscimento del grado di invalidita'

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 11 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento

copia informatica per consultazione

	dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (art. 403) - D.P.R. 24.07.1977, n. 616 - L. 5.02.1992, n. 104 - L. 8.11.2000, n. 328
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 11- Sistema informativo relativo all'attivita' relativa all'integrazione sociale ed all'istruzione di soggetti che versano in condizioni di disagio sociale e psico-sociale (centro diurno, centro socio educativo, ludoteca, ecc.) - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 11 - Trattamento effettuato per finalita' di diritti sociali, politiche sociali e famiglia: Interventi per la disabilita'. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 11 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: tutela sociale della maternita' ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili ai sensi dell'art. 2-sexies, comma 2 lett. aa) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (integrazione sociale ed istruzione del portatore di handicap)
Interesse legittimo	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in

copia informatica per consultazione

perseguito	forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 11 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) circoscrizioni, istituti scolastici, enti convenzionati (per l'erogazione dei servizi) b) centro servizi regionali (per lo scambio delle informazioni a fini di monitoraggio e rendicontazione)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Persone disabili - Minori di eta' - Scolari o studenti di ogni ordine e grado

copia informatica per consultazione

Categorie di destinatari	- Soggetti privati - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013

copia informatica per consultazione

Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

copia informatica per consultazione

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

copia informatica per consultazione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA'	Molto alto

copia informatica per consultazione

E GRAVITA' (rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Servizio di assistenza educativa alunni disabili in ambito scolastico

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO	Servizio Scuola e Biblioteca

TRATTAMENTO	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

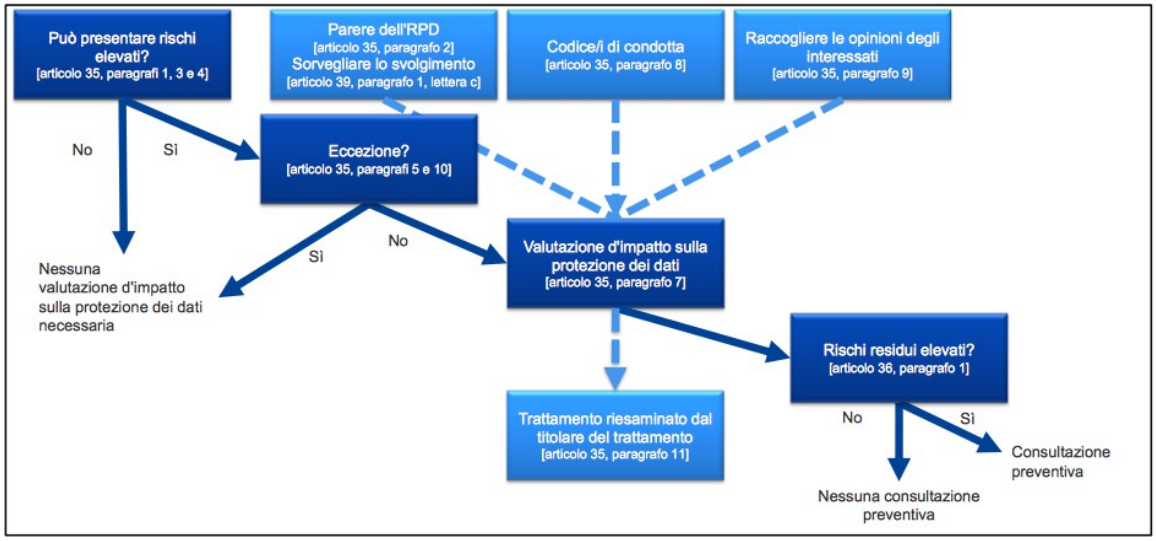
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

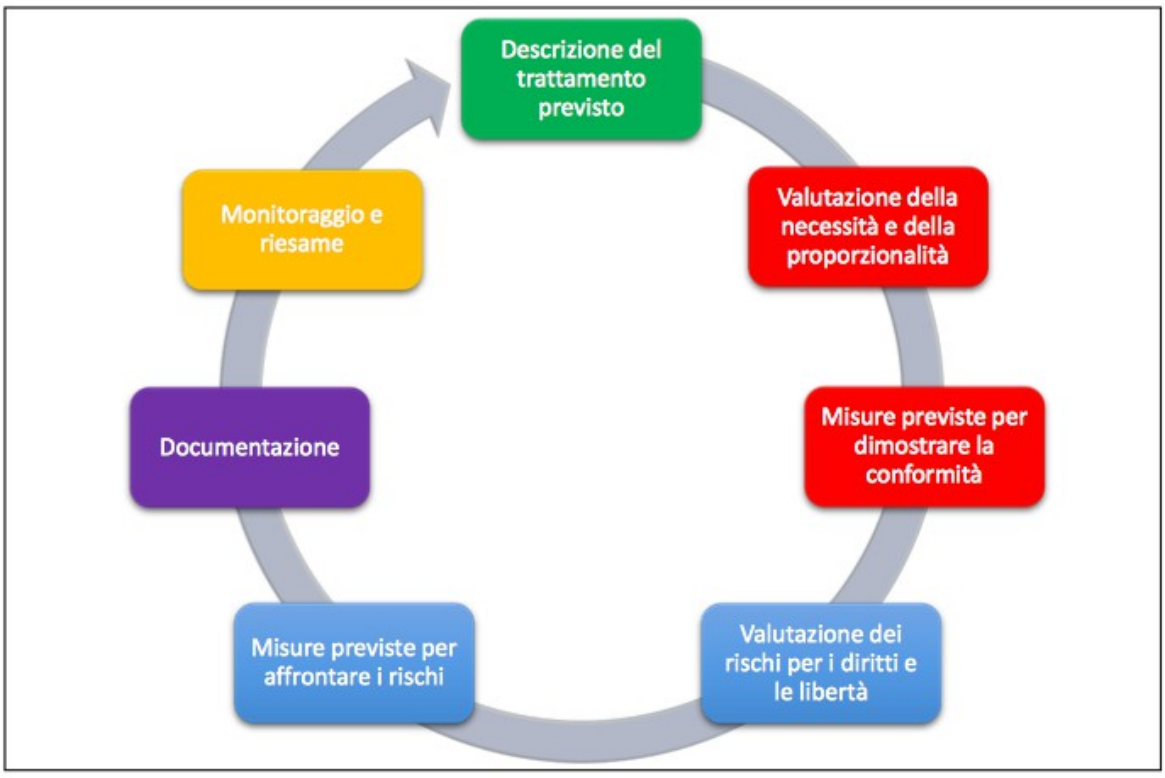
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO: denominazione e punti di contatto	Servizio Scuola e Biblioteca
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	Istituto Comprensivo G. Giusti Sistema Documentario Territoriale Livornese A.S.A. S.P.A. AZIENDA SERVIZI AMBIENTALI S.P.A.
Responsabile trattamento: denominazione e punti di contatto	LINC scs
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 14 - I dati vengono forniti dall'interessato, previa presentazione dell'istanza per accedere al contributo e/o al ricovero, ovvero da terzi (ASL o tutore, per predisporre una relazione di valutazione dello stato di non autosufficienza psico-fisica relativa all'interessato). Le informazioni sulla salute sono comunicate unicamente all'istituto che presso il quale viene effettuato il ricovero, in particolare viene comunicata l'ammissione del beneficiario, il grado di invalidita' e le particolari patologie dell'interessato, al fine di garantire un'assistenza mirata. Le eventuali convinzioni religiose e filosofiche possono invece rilevare ai fini dell'erogazione di particolari regimi alimentari. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 14 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 5.12.1992, n. 104 - D.Lgs. 31.03.1998, n. 112 e relative disposizioni di attuazione - D.Lgs. 18.08.2000, n. 267 - leggi regionali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 14 - Sistema informativo relativo a concessione di contributi, sussidi e benefici - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare lo stato di salute: anamnesi familiare
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 14 - Trattamento effettuato per finalita' relative ad attivita' socio-assistenziali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla

copia informatica per consultazione

	legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 14 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci ai sensi dell'art. 2-sexies, comma 2 lett. s) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' socio-assistenziali)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 14 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Istituto che fornisce la prestazione (ai sensi della l. n. 328/2000) - Altre amministrazioni ed enti pubblici - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Utenti (anche potenziali)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta

copia informatica per consultazione

	salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune

copia informatica per consultazione

	modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati* (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi

copia informatica per consultazione

	di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5

copia informatica per consultazione

	(CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti

copia informatica per consultazione

	- CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto	

copia informatica per consultazione

	con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita

copia informatica per consultazione

	l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di

copia informatica per consultazione

	ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Servizio di fornitura testi scolastici per alunni della scuola primaria
Concessione prestazioni agevolate (servizi educativi, socio-assistenziali, etc.)

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO	Servizio Scuola e Biblioteca

TRATTAMENTO	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

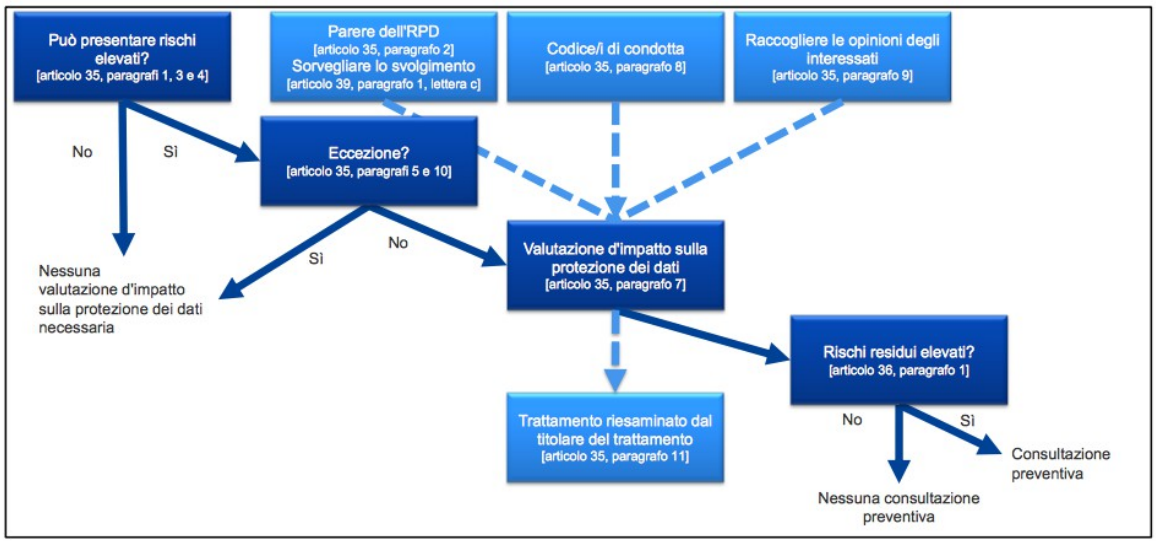
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

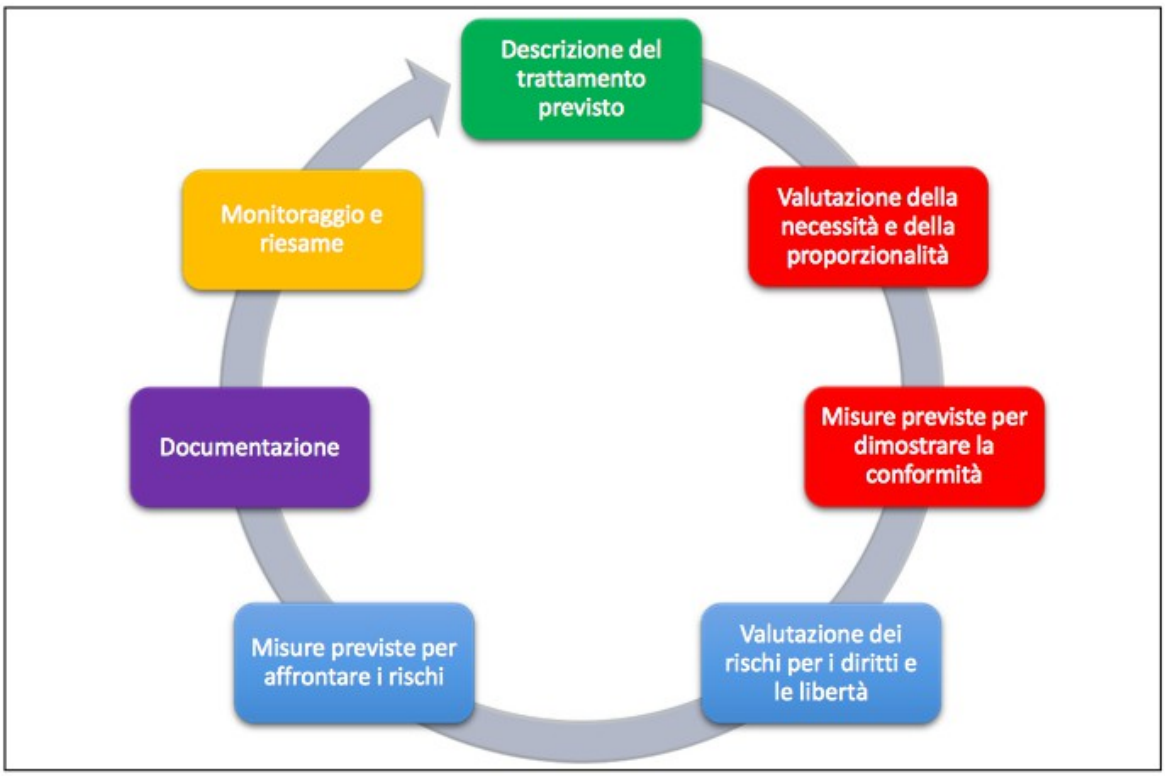
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO: denominazione e punti di contatto	Servizio Scuola e Biblioteca
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 21 - I dati sensibili degli alunni, relativi alle specifiche situazioni patologiche del minore, possono essere comunicati direttamente dalla famiglia. Inoltre, alcune particolari scelte per il servizio di mensa (pasti vegetariani o rispondenti a determinati dettami religiosi) possono essere idonee a rivelare le convinzioni (religiose, filosofiche o di altro genere) dei genitori degli alunni. Infine, il dato sull'origine etnica si potrebbe desumere dalla particolare nazionalita' dell'interessato. Le informazioni raccolte possono essere comunicate sia ad eventuali gestori esterni del servizio mense, che provvedono all'erogazione del servizio; sia a societa' che effettuano il servizio di trasporto scolastico.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 21 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 -

copia informatica per consultazione

	D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 6.12.1971, n. 1044 - D.Lgs. 31.03.1998, n. 112 (art. 139) - L. 5.02.1992, n. 104 (art. 13) - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016
Nome archivio/Banca dati	- Scheda n. 21 - Sistema informativo relativo ad asili nido e scuola - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 21 - Trattamento effettuato per finalita' relative a: gestione di asili nido e delle scuole per l'infanzia. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al

copia informatica per consultazione

	controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 21 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci ai sensi dell'art. 2-sexies, comma 2, lett. s), D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (gestione di asili nido e delle scuole per l'infanzia)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 21 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Gestori esterni delle mense e societa' di trasporto (per garantire l'erogazione del servizio)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Utenti (anche potenziali)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta

copia informatica per consultazione

	salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune

copia informatica per consultazione

	modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati* (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi

copia informatica per consultazione

	di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5

copia informatica per consultazione

	(CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti

copia informatica per consultazione

	- CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto	

copia informatica per consultazione

	con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita

copia informatica per consultazione

	l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di

copia informatica per consultazione

	ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Asili nido

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO	Servizio Scuola e Biblioteca

TRATTAMENTO	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

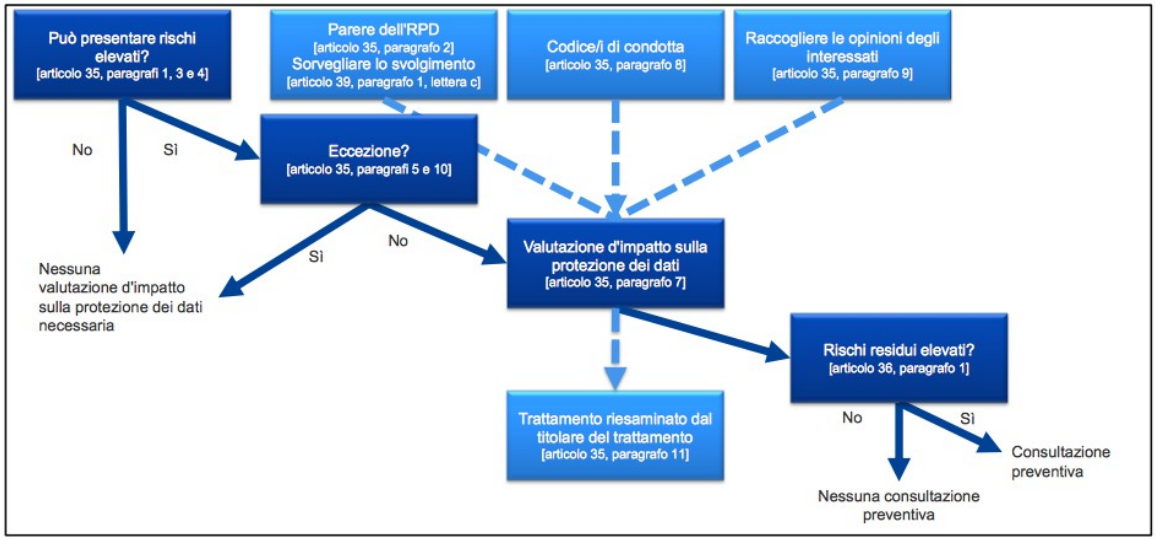
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

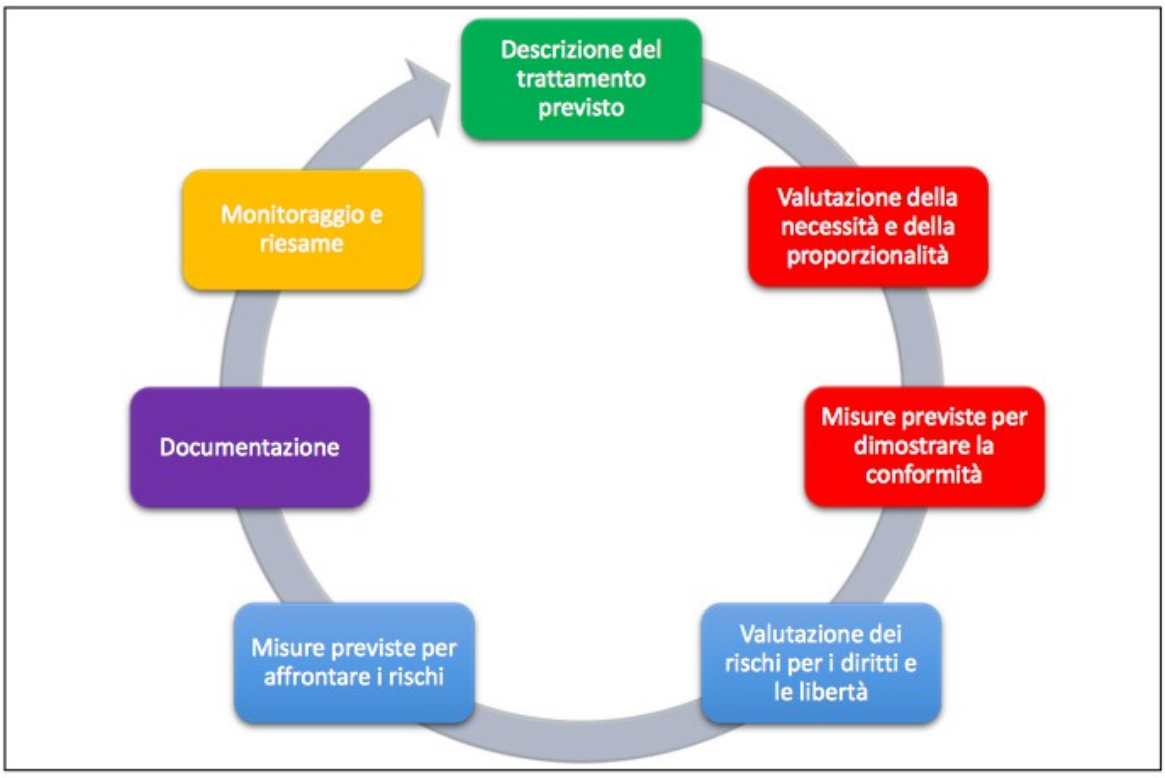
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO: denominazione e punti di contatto	Servizio Scuola e Biblioteca
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	Sistema Documentario Territoriale Livornese
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 37 - I dati vengono raccolti presso gli interessati i quali possono richiedere, per particolari iniziative, il patrocinio e/o l'erogazione di un contributo economico e/o la collaborazione dell'Amministrazione Comunale. Al fine di valutare eventuali cause ostative all'erogazione di un contributo, viene acquisita la posizione debitoria con una dichiarazione sostitutiva ai sensi degli artt. 46 e 47 del D.P.R. 445/2000. Altri dati sensibili possono emergere dagli Statuti delle associazioni, enti, fondazioni. Queste informazioni, eccetto quelle idonee a rivelare lo stato di salute, possono inoltre essere diffuse ai sensi del D.Lgs. n.267/2000 in ottemperanza al regime di pubblicita' degli atti (pubblicazioni Albo Pretorio). Con riferimento alle attivita' relative alla concessione di benefici, al riconoscimento di benefici il trattamento di dati sensibili si rende necessario sia per la concessione o l'assegnazione stesse, sia per la predisposizione delle graduatorie dei beneficiari, che vengono rese pubbliche ove previsto dalla relativa normativa, fermo restando il divieto di diffondere i dati sulla salute ai sensi degli artt. 22, comma 8, e 68, comma 3, del d.lgs. n. 196/2003. I dati vengono forniti direttamente dagli interessati, che presentano apposita domanda di contributo al Comune, oppure da terzi (anagrafe, autorita' giudiziaria, ASL, provincia, altri servizi comunali, i quali effettuano dei servizi di sostegno in favore dell'utente che versa in stato di indigenza).
Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente

copia informatica per consultazione

all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 37 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 3/3/1951, n.178; art.12 L.241/90; Regolamenti comunali in materia
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 37 - Sistema informativo relativo a concessione di onorificenze, ricompense, contributi, sussidi e benefici - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rivelare lo stato di disabilita'
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella

copia informatica per consultazione

	MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 37 - Trattamento effettuato per finalita' di diritti sociali, politiche sociali e famiglia. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 37 - Trattamento effettuato per rilevanti finalita' nella seguente materia: conferimento di onorificenze e ricompense, riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali ai sensi dell'art. 2-sexies, comma 2 lett. n) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 37 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): istanti, beneficiari (ai sensi del Regolamento per la concessione di contributi e delle normative nello stesso richiamate)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti -	

copia informatica per consultazione

particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Persone disabili - Persone fisiche - Persone in cerca di occupazione - Soggetti in difficolta' o pericolo (anche potenziali) - Soggetti con limitata capacita' di intendere e volere - Scolari o studenti di ogni ordine e grado - Rifugiati
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione	- I dati sono conservati in una forma che consente l'identificazione dell'interessato

copia informatica per consultazione

trattamento: *Periodo di conservazione dei dati*	per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia

copia informatica per consultazione

	effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita'***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei

copia informatica per consultazione

dei dati (rilevati dalla prospettiva degli interessati)	software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI

copia informatica per consultazione

	AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I

copia informatica per consultazione

	MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi,	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli

copia informatica per consultazione

modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

copia informatica per consultazione

- **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle	

copia informatica per consultazione

	informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

	- MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e

copia informatica per consultazione

	formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessione contributo a istituti scolastici paritari
Concessione contributo regionale buono-libri

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO	Servizio Scuola e Biblioteca

TRATTAMENTO	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

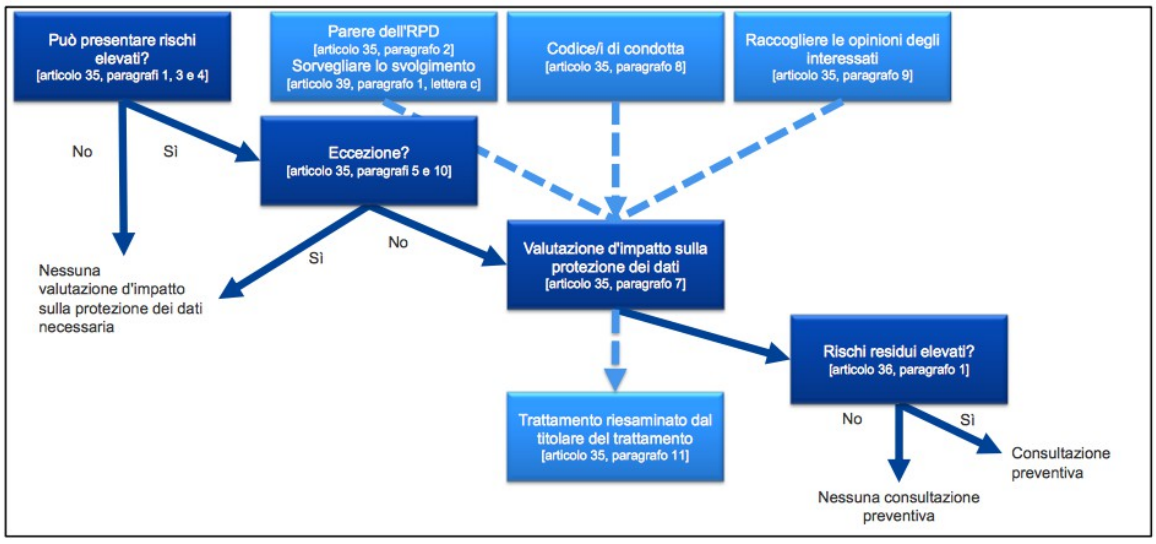
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

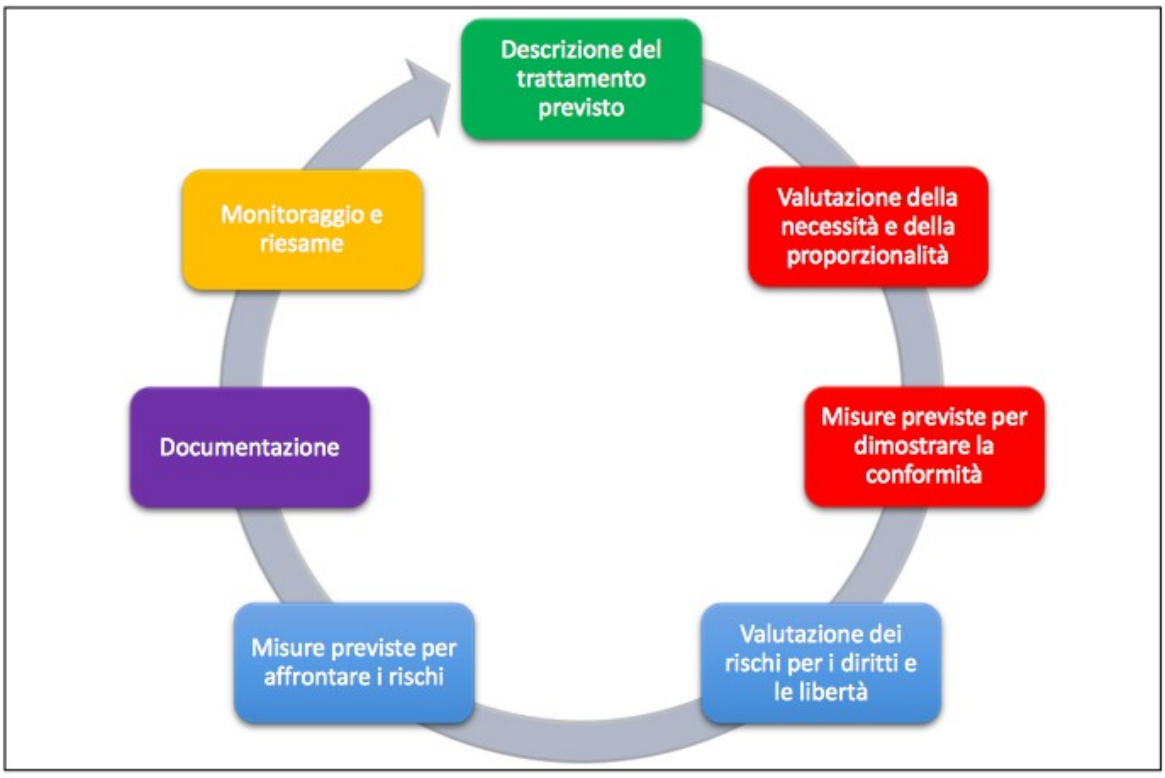
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SCUOLA E BIBLIOTECA
SERVIZIO: denominazione e punti di contatto	Servizio Scuola e Biblioteca
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	Istituto Comprensivo G. Giusti Scuola Dell'Infanzia V.T. Battaglini
Responsabile trattamento: denominazione e punti di contatto	Soggetto affidatario del servizio di assistenza alunni con disabilita' Soggetto affidatario del servizio di refezione scolastica Cooperativa Italiana di Ristorazione s.c. Itaca Societa' Cooperativa a.r.l.
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 50 - Il trattamento ha per oggetto i dati delle procedure di affidamento e dei contratti di appalto e di concessione delle amministrazioni aggiudicatrici e degli enti aggiudicatori per l'acquisizione di servizi, forniture, lavori e opere, nonche' i concorsi pubblici di progettazione e l'attivita' posta in essere in attuazione del D.Lgs. n. 50/2016. I dati vengono raccolti dai soggetti partecipanti alle procedure di affidamento e includono dati sensibili e giudiziari. Il trattamento implica, oltre alle ordinarie forme di elaborazione standardizzate (con mezzi elettronici e su supporto cartaceo), anche la comunicazione a terzi e, in particolare, alle Autorita' competenti a rilasciare le certificazioni sul possesso dei requisiti, nonche' la possibile diffusione mediante pubblicazione sul profilo del committente e sui siti web prescritti dalla normativa vigente in materia.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 50 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001- Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 50/2016 - Linee Guida Anac - Statuto - Regolamento sul procedimento amministrativo - Regolamento sull'attivita' contrattuale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza trasversalmente, di tutti gli uffici che aggiudicano contratti inclusi nell'ambito di applicazione del D.Lgs. 50 n. 0/2016
Nome archivio/Banca dati	- Scheda n. 50 - Sistema informativo relativo ad appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili - Dati relativi al comportamento debitorio - Dati relativi all'affidabilita' o puntualita' nei pagamenti - Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati relativi all'adempimento di obbligazioni - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti - Dati relativi all'affidabilita' nell'esecuzione dei contratti pubblici
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi

copia informatica per consultazione

Finalita' del trattamento	- Scheda n. 50 - Trattamento effettuato per finalita' di adempimento di obblighi contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 50 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 50 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Agenzia Entrate, Prefettura, Tribunale, Procura presso il Tribunale, Provincia e altri enti pubblici - INPS/INAIL/ANAC - , anche attraverso la consultazione delle relative Banche dati, per i controlli sul possesso dei requisiti dichiarati in sede di procedura di affidamento; b) altri soggetti partecipanti alla procedura di affidamento; c) consulenti e soggetti, pubblici o privati, che effettuano servizi di committenza ausiliaria; d) avvocati incaricati dell'eventuale contenzioso (ai sensi del D.Lgs. n. 50/2016 e della regolazione attuativa)
Categorie di trattamenti - particolari forme di elaborazione:	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione sul sito web, in "Amministratrazione trasparente" in attuazione di obblighi di pubblicazione di cui al D. Lgs. n. 33/2013

copia informatica per consultazione

diffusione	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Concorrenti alle procedure di affidamento di contratti pubblici - Soggetti terzi rispetto ai concorrenti, i cui dati rilevano nella procedura di affidamento
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

cartacei o canali di trasmissione	
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II

copia informatica per consultazione

VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la

copia informatica per consultazione

	consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

RISCHI **Origine/fonte dei rischi:** ***accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle

copia informatica per consultazione

	password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC

copia informatica per consultazione

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

copia informatica per consultazione

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare	

copia informatica per consultazione

	l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto

copia informatica per consultazione

	- MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione:

copia informatica per consultazione

	FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio pre e post scuola
Servizio di ristorazione scolastica
Servizio di trasporto scolastico

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA E PROTOCOLLO
SERVIZIO	Servizio Segreteria e Protocollo

TRATTAMENTO	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

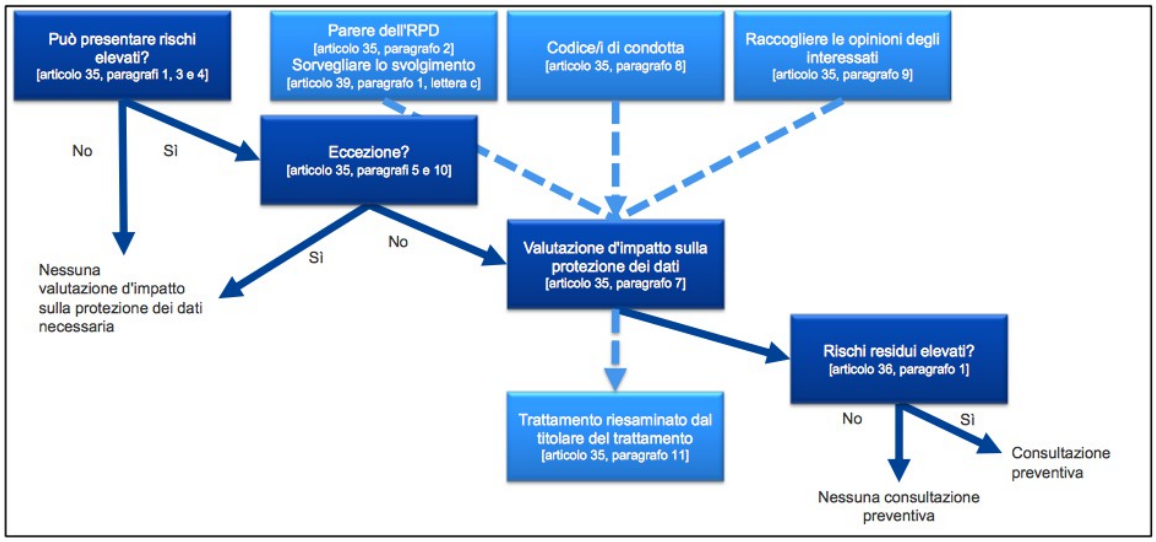
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

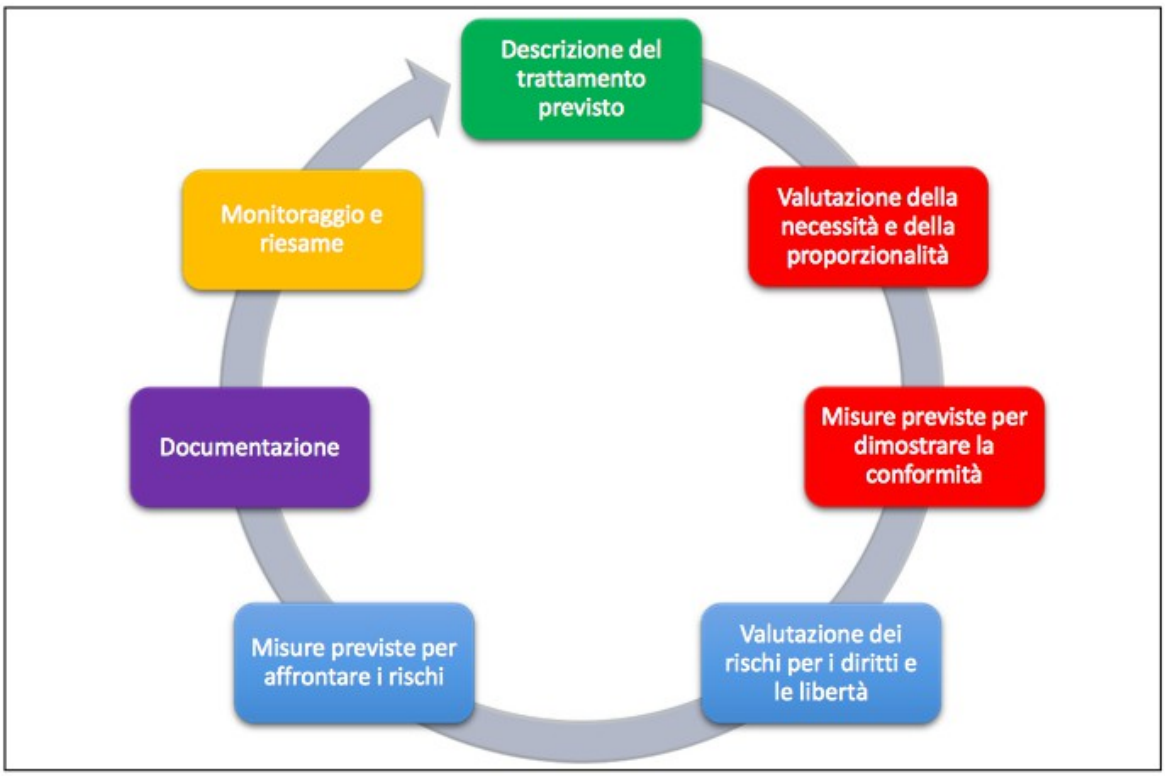
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA E PROTOCOLLO
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria e Protocollo
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Infoelba s.r.l. Elba Informatica s.a.s. Apkappa s.r.l. Next Step Solution s.r.l. Datagraph s.r.l. Maggioli S.p.A.
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig.ra Raino' Chiara Sig.ra Rossi Carla

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 59 - I dati vengono nella gestione della rete informatica, dell'hardware e dei server, in relazione a dati personali in particolare dei dipendenti pubblici che utilizzano gli strumenti e degli utenti esterni che accedono alla rete.
Il trattamento puo' includere anche dati comuni e sensibili. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici, tramite sistema informativo, assistenza informatica, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n.114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 59 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 59 - Base di dati: sistema informativo, assistenza informatica, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di accesso e di identificazione (user name, password, customer ID, altro)
Luoghi di custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 59 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 59 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico,inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti)

copia informatica per consultazione

Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Utenti (anche potenziali)

copia informatica per consultazione

Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione

copia informatica per consultazione

Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizi di disaster recovery e backup
Servizi di gestione hardware e software
Assistenza utenti: Interventi supporto per la gestione dati applicativi

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA E PROTOCOLLO
SERVIZIO	Servizio Segreteria e Protocollo

TRATTAMENTO	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

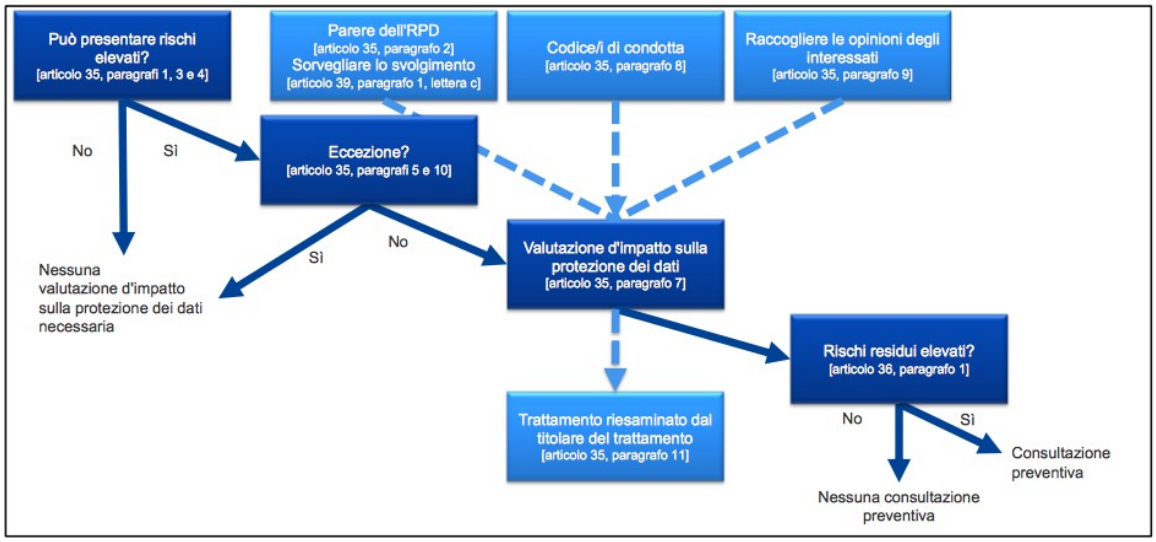
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

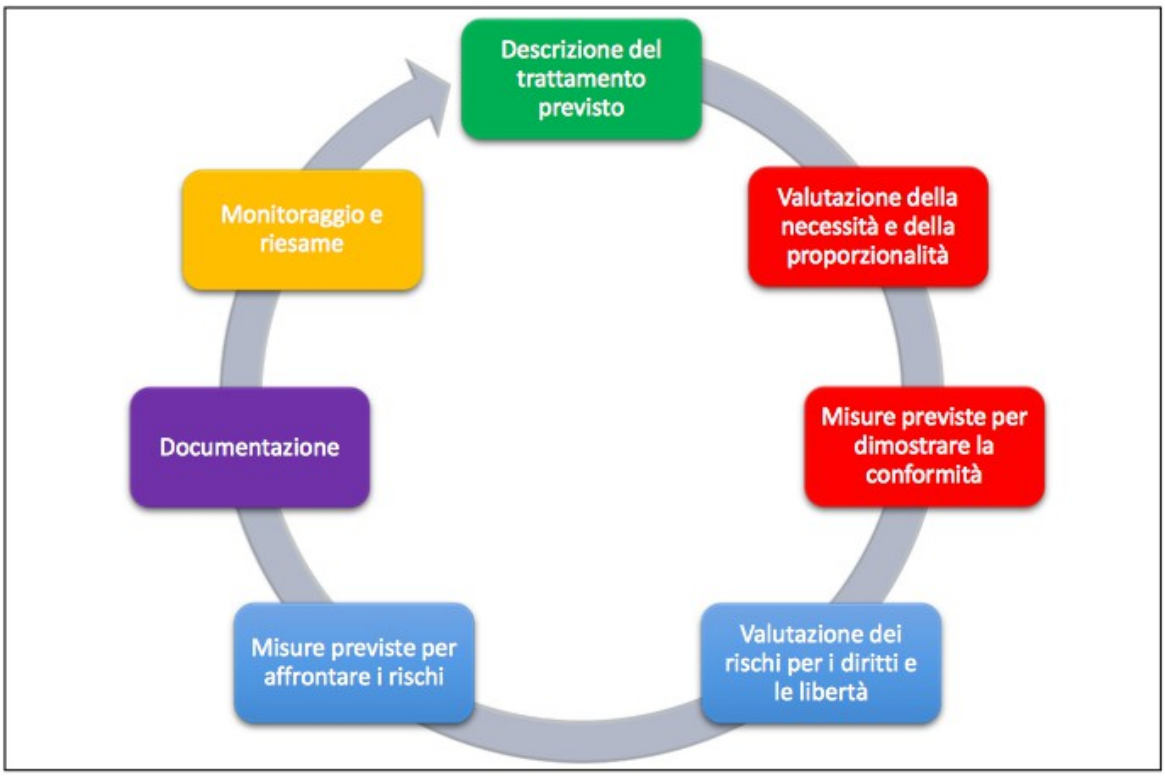
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA E PROTOCOLLO
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria e Protocollo
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	sig.ra Raino' Chiara Sig.ra Rossi Carla

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 61 - I dati vengono raccolti dall'Ufficio Segreteria e protocollo sia presso l'ente, sia presso terzi, sia presso gli interessati. Il trattamento (che include anche dati vulnerabili e sensibili) e' effettuato per rilevanti finalita' di interesse pubblico relative verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo tramite sistema informativo, protocollo interno, raccolta pratiche, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n.114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 61 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000

copia informatica per consultazione

	- D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 61 - Sistema informativo relativo al protocollo interno e raccolta pratiche - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 61 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 61 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: volgimento delle funzioni di controllo, indirizzo politico,inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di

copia informatica per consultazione

	razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	

copia informatica per consultazione

Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto

copia informatica per consultazione

Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Pubblicazione delle deliberazioni
Gestione del protocollo
Gestione dell'archivio corrente e di deposito

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

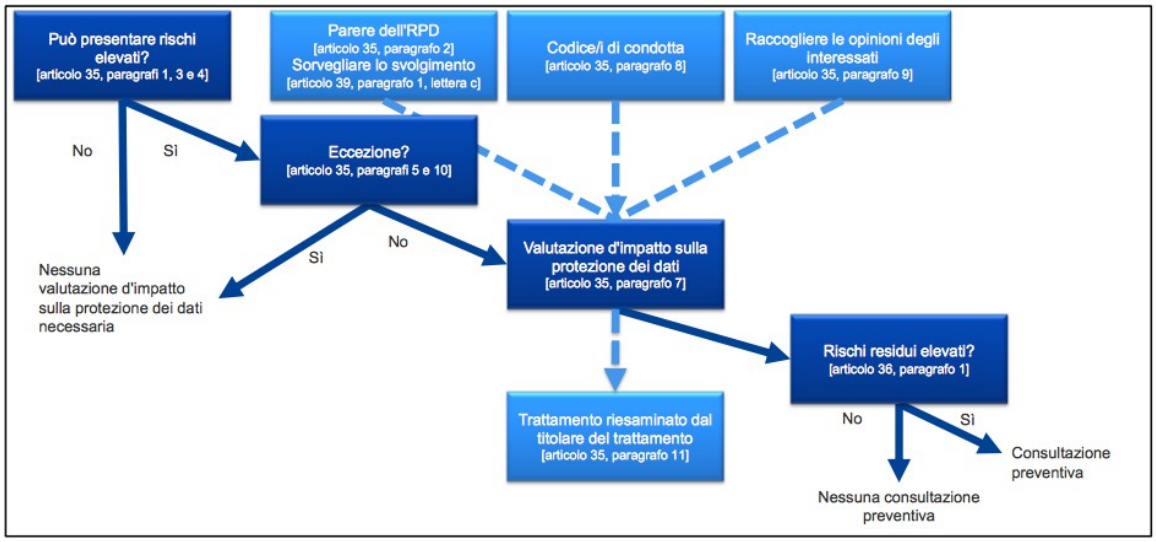
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

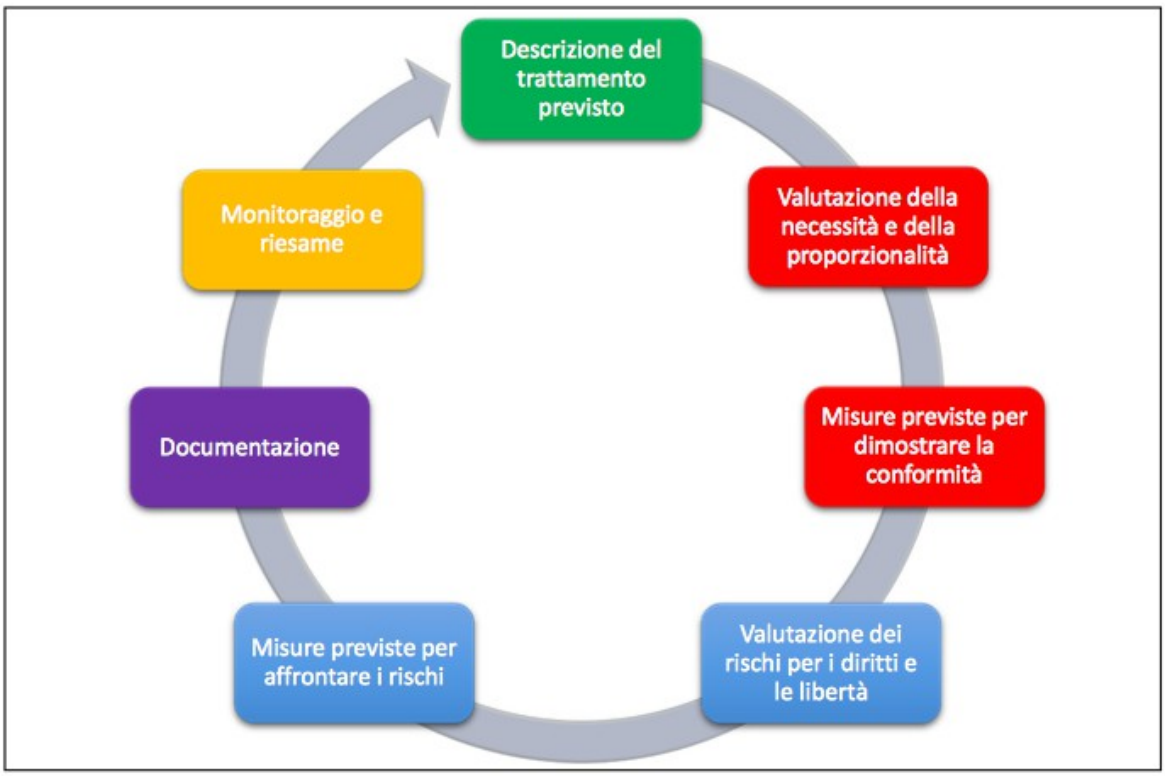
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 01 - Il trattamento concerne tutti i dati relativi all'instaurazione ed alla gestione del rapporto di lavoro, avviato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'ente ovvero in aziende o istituzioni collegate o vigilate, a partire dai procedimenti concorsuali o da altre procedure di selezione. I dati sono oggetto di trattamento presso le competenti strutture del Comune per quanto riguarda la gestione dell'orario di servizio, le certificazioni di malattie ed altri giustificativi delle assenze; vengono inoltre effettuati trattamenti a fini statistici e di controllo di gestione. I dati sulle convinzioni religiose possono rendersi necessari per la concessione di permessi per quelle festivita' la cui fruizione e' connessa all'appartenenza a determinate confessioni religiose; quelli sulle opinioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza o in relazione a particolari preferenze alimentari, laddove e' previsto un servizio di mensa; le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso. Possono essere raccolti anche dati sulla salute relativi ai familiari del dipendente ai fini della concessione di benefici nei soli casi previsti dalla legge. I dati pervengono su iniziativa dei dipendenti e/o previa richiesta da parte del Comune. I dati vengono trattati ai fini dell'applicazione dei vari istituti contrattuali disciplinati dalla legge (gestione giuridica, economica, previdenziale, pensionistica, attivita' di aggiornamento e formazione). Vengono effettuate interconnessioni e raffronti con amministrazioni

copia informatica per consultazione

e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 01 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (artt. 2094 - 2134) - D.P.R. 30.06.1965, n. 1124 - L. 20.05.1970, n. 300 - L. 7.02.1990, n. 19 - D.Lgs. 19.09.1994, n. 626 - L. 12.03.1999, n. 68 - Legge 8.03.2000, n. 53 - D.Lgs. 18.08.2000, n. 267 - D.Lgs. 30.03.2001, n. 165 - D.Lgs. 26.03.2001, n. 151 - L. 6.03.2001, n. 64 - D.P.R. 28.12.2000, n. 445 - D.Lgs. 15.08.1991, n. 277 - L. 14.04.1982, n. 164 - CCNL - Contratto collettivo decentrato di ogni singolo ente - Regolamenti comunali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 01 - Sistema informativo relativo alla gestione rapporti contrattuali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rivelare la vita sessuale (soltanto in caso di rettificazione di sesso) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali

copia informatica per consultazione

	- Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 01 - Trattamento effettuato per finalita' di gestione del rapporto di lavoro in tutte le sue fasi. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 01 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva ai sensi dell'art. 2-sexies, comma 2 lett. dd) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 01 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) alle organizzazioni sindacali ai fini della gestione dei permessi e delle trattenute sindacali relativamente ai dipendenti che hanno rilasciato delega; b) enti assistenziali, previdenziali e assicurativi e autorita' locali di pubblica sicurezza a fini assistenziali e previdenziali, nonche' per rilevazione di eventuali patologie o infortuni sul lavoro; c) alla Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (d.lgs. n. 165/2001);

copia informatica per consultazione

	d) uffici competenti per il collocamento mirato, relativamente ai dati anagrafici degli assunti appartenenti alle "categorie protette"; e) strutture sanitarie competenti per le visite fiscali (art. 5, l. n. 300/1970 e CCNL); f) enti di appartenenza dei lavoratori comandati in entrata (per definire il trattamento retributivo del dipendente); g) Ministero economia e finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600); h) ISPELS (ax art. 70 d.lgs. n. 626/1994)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Personale dipendente - Collaboratori
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che

copia informatica per consultazione

dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

copia informatica per consultazione

dati personali	

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico,

copia informatica per consultazione

	ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche

copia informatica per consultazione

	amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha

copia informatica per consultazione

illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

copia informatica per consultazione

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di	

copia informatica per consultazione

	amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione

copia informatica per consultazione

	dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

copia informatica per consultazione

delle misure	

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Selezione per l'affidamento di incarichi professionali
Partecipazione a coordinamenti intercomunali
Registro dei responsabili del trattamento relativo alle attivita' di trattamento dei dati personali
Registro del titolare del trattamento dei dati personali

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

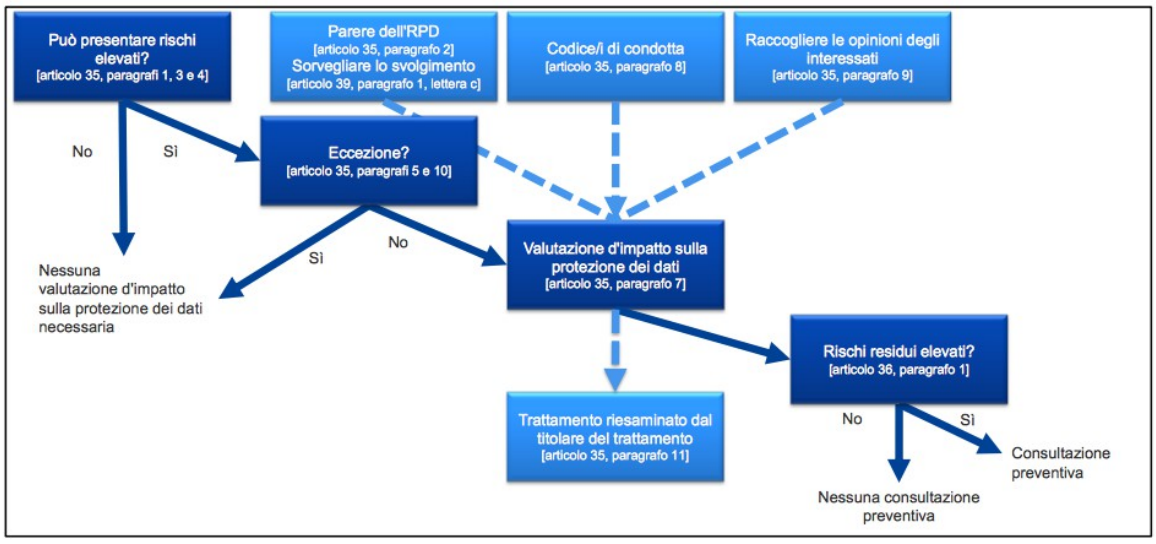
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

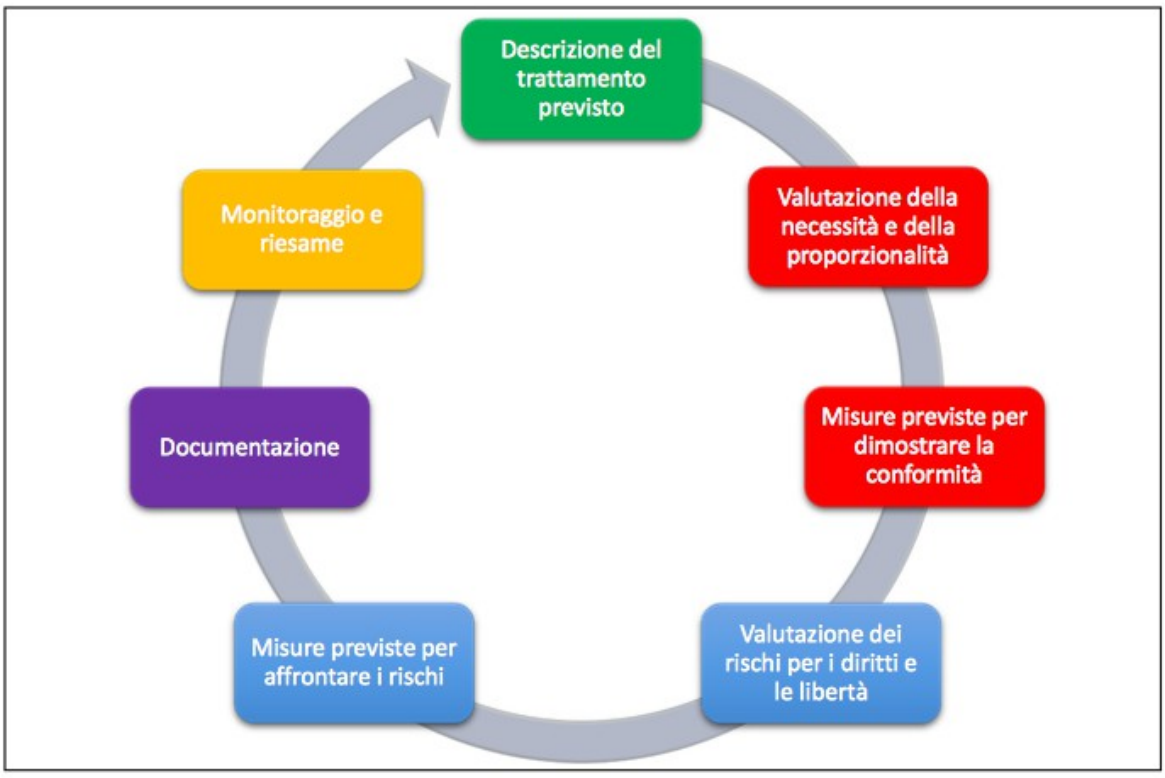
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 02 - I dati vengono acquisiti dall'interessato e da terzi previa richiesta dell'interessato (in particolare dalla Commissione medico ospedaliera territorialmente competente per l'accertamento delle condizioni di idoneita' al servizio e dal Comitato di verifica per le cause di servizio in caso di richiesta di riconoscimento di invalidita' dipendente da causa di servizio e/o equo indennizzo). In caso di richiesta di pensione privilegiata, i dati vengono trasmessi all'Inpdap per l'erogazione del trattamento pensionistico. Uguale trasmissione si ha nell'ipotesi di richiesta di riconoscimento alla contribuzione figurativa di cui all'art. 80, l. n. 388/2000. Esperita l'istruttoria, la determinazione dirigenziale relativa al riconoscimento dell'invalidita' viene comunicata all'INPS o alle Regioni (per gli accertamenti connessi alla liquidazione ai sensi dell'art. 130 d.lg. n. 112/1998). Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 02 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.P.R. 30.06.1965, n. 1124 - L. 24.05.1970, n. 336 - Legge 5.02.1992, n. 104 - L. 12.03.1999, n. 68 - D.P.R. 29.10.2001, n. 461 - L. 8.08.1995, n. 335 - L. 8.03. 1968, n. 152 - Legge regionale - regolamento comunale in materia di organizzazione del personale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 02 - Base di dati: sistema informativo gestione giuridica del personale, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 02 - Trattamento effettuato per finalita' di gestione del rapporto di lavoro in tutte le sue fasi. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati

copia informatica per consultazione

	possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 02 - Trattamento effettuato per rilevanti finalita' di interesse pubbliconella seguente materia: concessione, liquidazione modifica e revoca di benefici economici, agevolazioni, elargizioni, emolumenti ai sensi dell'art. 2-sexies, comma 2 lett. m) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 02 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) INAIL (per verificare la liquidazione in caso di equo indennizzo ai sensi del d.P.R. n. 1124/1965); b) comitato di verifica per le cause di servizio e commissione medica territorialmente competente (per conseguire il parere definitivo di riconoscimento della causa di servizio ai sensi del d.P.R. n. 461/2001); c) INPDAP (in caso di inabilita' assoluta e permanente a qualsiasi attivita' lavorativa ai fini dell'erogazione del relativo trattamento di pensione e del riconoscimento del diritto alla pensione privilegiata ai sensi della l. n. 335/1995 e della l. n. 152/1968)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome*	

copia informatica per consultazione

del dominio del sito web	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Personale dipendente - Dirigenti e dipendenti
Categorie di destinatari	- Organismi del servizio sanitario nazionale - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della

copia informatica per consultazione

	conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita'

copia informatica per consultazione

	- Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati* (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

copia informatica per consultazione

	VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di

copia informatica per consultazione

	trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici	

copia informatica per consultazione

	MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

copia informatica per consultazione

	- MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Denunce infortuni sul lavoro

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

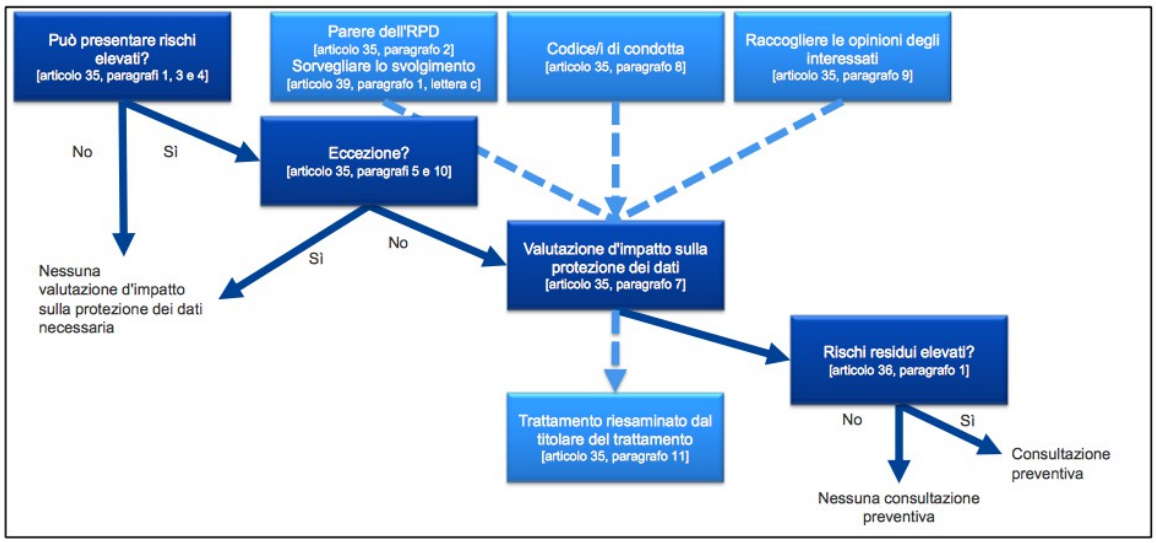
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

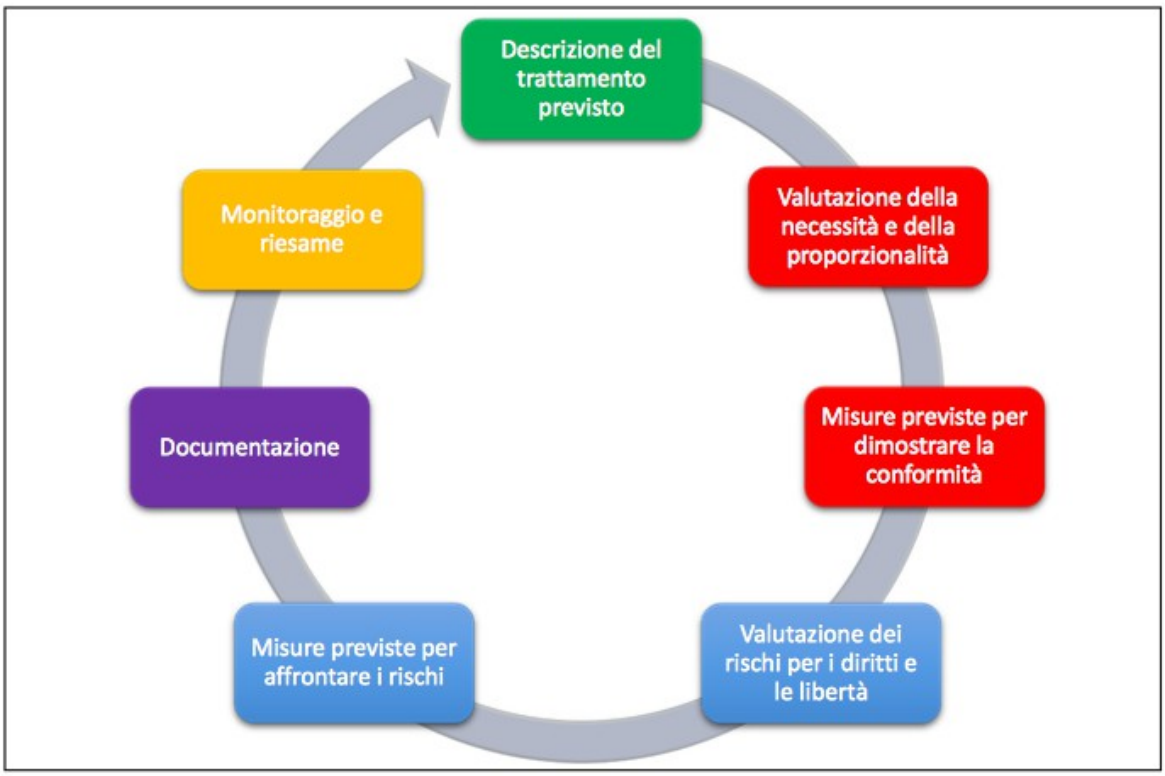
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 31 - Il trattamento concerne tutti i dati utili ad inserire gli utenti in un percorso di orientamento/formazione all'occupazione; i dati possono essere altresi' utilizzati per la predisposizione di corsi di formazione, tirocini o colloqui di orientamento. I dati pervengono dagli interessati ovvero sono raccolti su sua richiesta da terzi. Possono essere effettuati interconnessioni con la provincia, la regione e gli operatori pubblici e privati ai fini dell'attuazione della disciplina in materia di collocamento e mercato del lavoro. I dati, inoltre, vengono comunicati a centri di formazione professionale, associazioni e cooperative del terzo settore ed aziende che gestiscono programmi di inserimento al lavoro o di formazione ai fini dell'attuazione della disciplina in materia di formazione professionale.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Fonte normativa	- Scheda n. 31 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 8.11.1991, n. 381 - L. 24.06.1997, n. 196 - D.Lgs. 23.12.1997, n. 469 - L. 12.03.1999, n. 68 - L. 17.05.1999, n. 144 - L. 20.02.2003, n. 30 - D.Lgs. 10.09.2003, n. 276 - D.Lgs. 31.03.1998, n. 112 - D.Lgs. 21.04.2000, n. 181 - D.Lgs. 15.04.2005, n. 76 - D.Lgs. 25.07.1998, n. 286 - Leggi regionali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 31 - Base di dati: sistema informativo, inquadramenti e applicazione contratti collettivi di lavoro, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 31 - Trattamento effettuato per finalita' relative a: supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare

copia informatica per consultazione

Rilevanti finalita' di interesse pubblico	- Scheda n. 31 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva ai sensi dell'art. 2-sexies, comma 2 lett. dd) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 31 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): centri di formazione professionale, associazioni e cooperative terzo settore, aziende per inserimento al lavoro o alla formazione (limitatamente alle informazioni indispensabili all'instaurazione del rapporto di lavoro) - Altre amministrazioni ed enti pubblici - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E. - Candidati a scrutatori o presidenti di seggio
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

conservazione dei dati	
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i

copia informatica per consultazione

	parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks

copia informatica per consultazione

indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare
  3 = alto = = e' **probabile** che la minaccia si possa verificare
  4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da

copia informatica per consultazione

un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la	

copia informatica per consultazione

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile	Soggetto individuato in base agli atti di organizzazione

copia informatica per consultazione

attuazione misure	

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Verifica delle offerte anomale art. 97

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

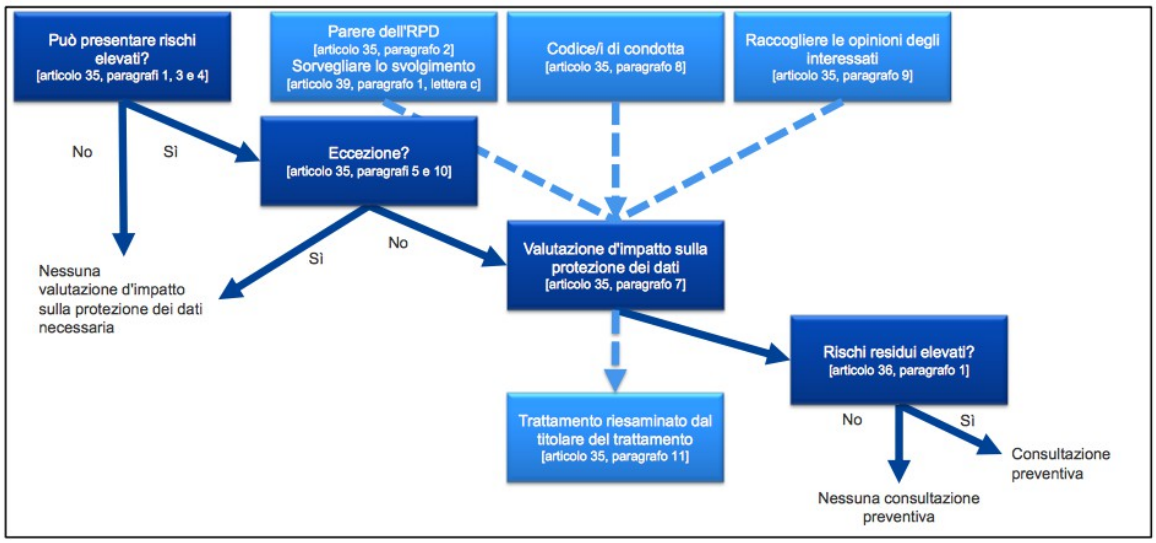
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

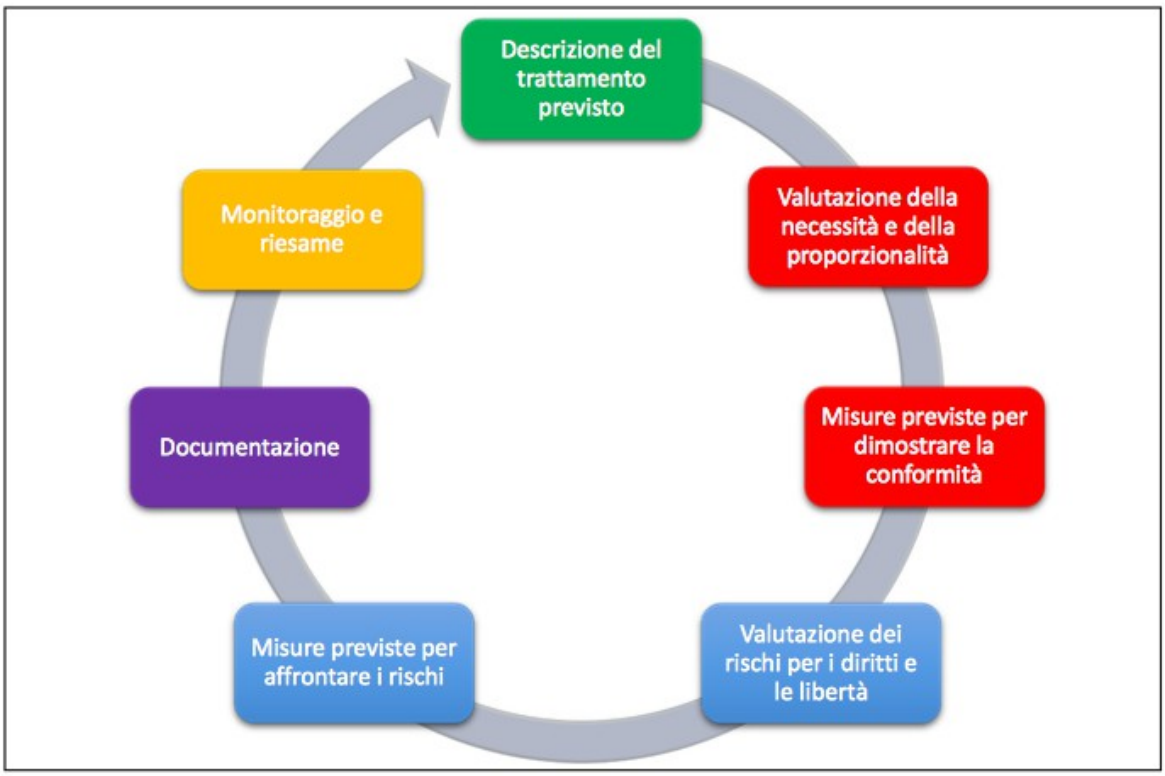
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 32 - Al fine di valutare eventuali cause ostative alla candidatura dei singoli soggetti, cosi' come per la pronuncia di decadenza di diritto (preventiva o successiva) dall'incarico, vengono acquisiti i dati giudiziari dalla Procura della Repubblica, dall'Ufficio elettorale centrale presso il Tribunale, dalla Prefettura e dal Ministero dell'Interno. Le decisioni in materia di candidabilita', contenenti in particolare la sigla politica di appartenenza dell'interessato, vengono pubblicate all'albo pretorio. Oltre alle informazioni di carattere politico, sindacale, religioso e di altro genere, il comune tratta i dati sanitari degli organi istituzionali al fine di verificare la loro partecipazione alle attivita' dell'ente. I dati vengono diffusi nei casi previsti dalla normativa in vigore (pubblicazione all'albo pretorio delle decisioni in materia di candidabilita' ai sensi d.lgs. n. 267/2000; pubblicita' dell'anagrafe degli amministratori locali ai sensi del citato d.lgs. n. 267/2000). Con riferimento alla nomina del difensore civico, la valutazione del dato politico e giudiziario, in relazione alla presentazione dei curricula, avviene sia a livello politico (da parte dei gruppi consiliari e dei relativi uffici di supporto), sia a livello amministrativo (da parte degli organi del comune, deputati all'istruttoria e alla verifica dei requisiti soggettivi e oggettivi). Il trattamento e' altresi' finalizzato all'accertamento dei requisiti di professionalita' ed onorabilita' dei candidati alle nomine presso enti, aziende e istituzioni. Le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso.

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 32 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 18.08.2000, n. 267 (artt. 55 e ss.) - L. 25.03.1993, n. 81 - L. 30.04.1999, n. 120 - L. 5.07.1982, n. 441 - D.P.R. 16.05.1960, n. 570 - L. 19.03.1990, n. 55 (art. 15) - L. 14.04.1982, n. 164
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 32 - Sistema informativo relativo agli organi istituzionali dell'ente - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rivelare la vita sessuale (soltanto in caso di eventuale rettificazione di attribuzione di sesso)
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi

copia informatica per consultazione

Finalita' del trattamento	- Scheda n. 32 - Trattamento effettuato per finalita' relative all'applicazione della disciplina in materia di elettorato attivo e passivo, esercizio del mandato degli organi rappresentativi e di affidamento di incarichi di rappresentanza in enti, aziende e istituzioni nonche' accertamento dei requisiti di onorabilita' e di professionalita' per le nomine a cariche direttive di persone giuridiche. Finalita' ulteriore rispetto a quella per la quale sono raccolti i dati: pagamento emolumenti agli amministratori
Rilevanti finalita' di interesse pubblico	- Scheda n. 32 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: esercizio del mandato degli organi rappresentativi, ivicompresa la loro sospensione o il loro scioglimento, nonche' l'accertamento delle cause di ineleggibilita', incompatibilita' o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche (art. 2-sexies, comma 2 lett. g) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (applicazione della disciplina in materia di elettorato attivo e passivo, esercizio del mandato degli organi rappresentativi e di affidamento di incarichi di rappresentanza in enti, aziende e istituzioni nonche' accertamento dei requisiti di onorabilita' e di professionalita' per le nomine a cariche direttive di persone giuridiche, e pagamento emolumenti agli amministratori)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 32 - Ministero economia e finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n.164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600) e al Ministero dell'Interno per l'anagrafe degli amministratori locali (ex art. 76 d.lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa):imitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio delle decisioni in materia di candidabilita' (D.Lgs. n. 267/2000) e di anagrafe degli amministratori locali (D.Lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite*	

copia informatica per consultazione

un sito web-nome del dominio del sito web	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Amministratori
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non

copia informatica per consultazione

delle diverse categorie di dati	superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi

copia informatica per consultazione

trattamento in relazione alle finalita'	informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

copia informatica per consultazione

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con

copia informatica per consultazione

	violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la

copia informatica per consultazione

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione

copia informatica per consultazione

	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X	Medio

copia informatica per consultazione

(rilevata dalla prospettiva degli interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che

copia informatica per consultazione

fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	

copia informatica per consultazione

Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della

copia informatica per consultazione

	sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame,

copia informatica per consultazione

	documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Agenda Sindaco ed Assessori
Assistenza organi istituzionali: Gestione sedute commissioni consiliari
Assistenza organi istituzionali: Gestione sedute conferenze capigruppo
Assistenza organi istituzionali: Gestione sedute Consiglio comunale
Assistenza organi istituzionali: Trascrizione verbali consiglio
Assistenza organi istituzionali: Surroghe
Assistenza organi istituzionali: Convalida consiglieri
Funzionamento degli organi collegiali
Assistenza organi istituzionali: Nomina Presidente e vicepresidenti
Assistenza organi istituzionali: Decadenze
Assistenza organi istituzionali: Fornitura servizi ai gruppi consiliari
Assistenza organi istituzionali: Gestione sedute Giunta comunale
Anagrafe degli eletti: Pubblicazione e aggiornamento dati on line
Designazione dei rappresentanti dell'ente presso enti, societa', fondazioni

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

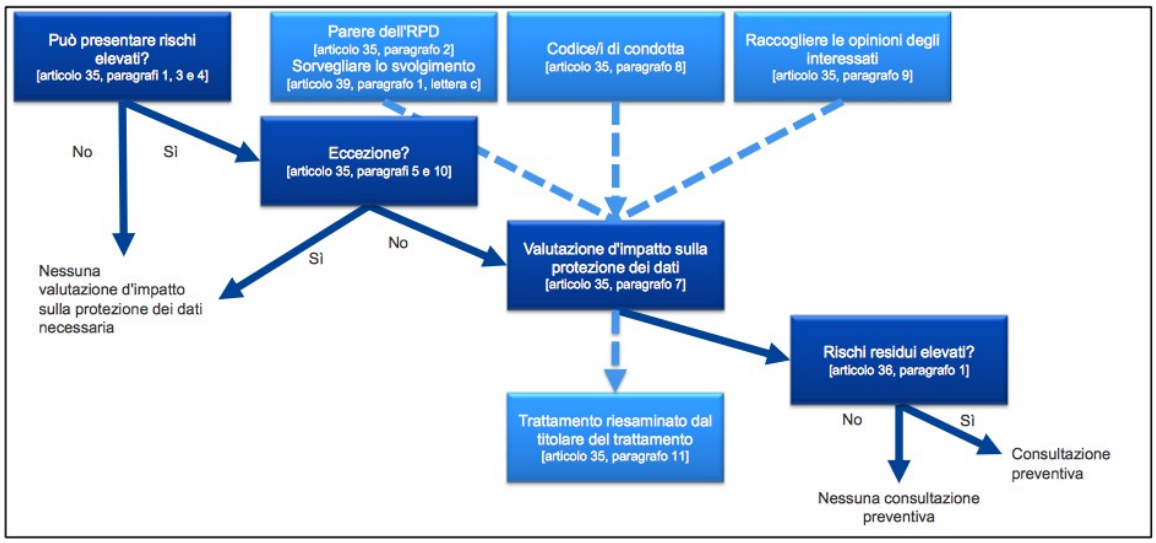
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

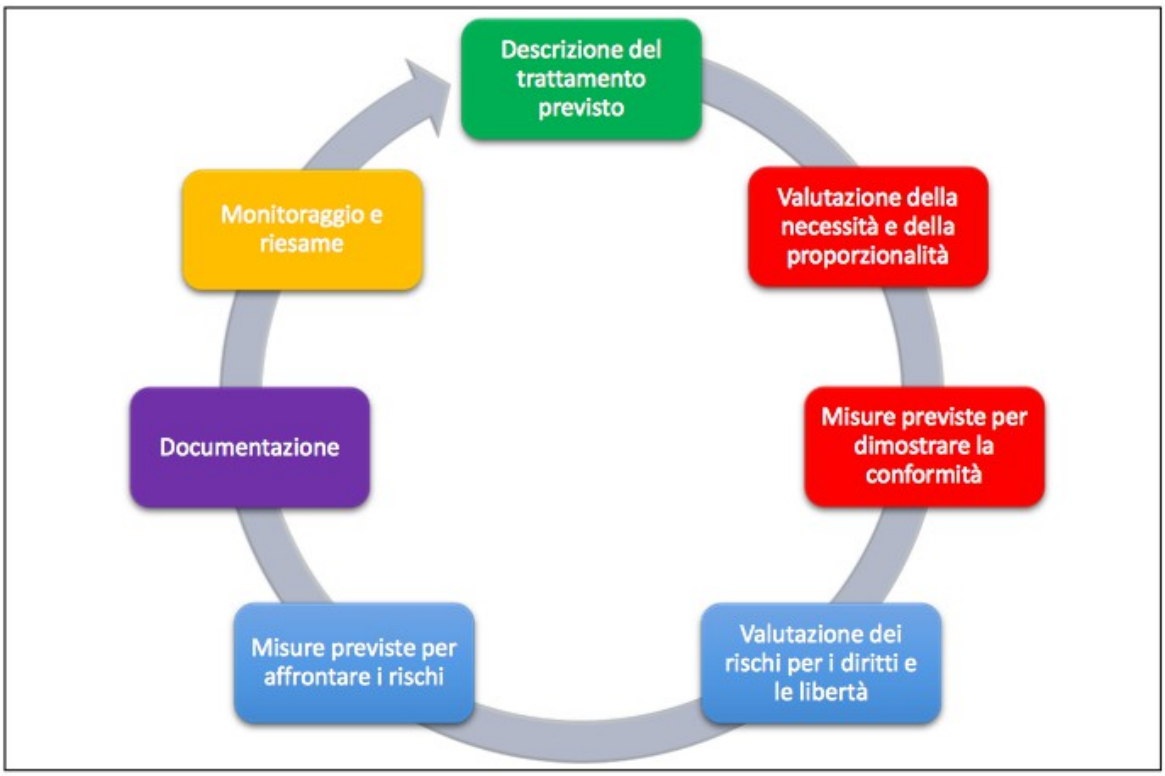
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 33 - Nell'ambito delle proprie prerogative, i consiglieri comunali e gli amministratori possono formulare atti sia di indirizzo politico (quali mozioni, ordini del giorno e risoluzioni), sia di sindacato ispettivo (presentando interrogazioni ed interpellanze alla Giunta comunale), secondo le modalita' stabilite dallo Statuto dal regolamento interno del Consiglio comunale. Le predette attivita' possono comportare il trattamento di dati sensibili e giudiziari riguardanti le persone oggetto di mozioni, ordini del giorno, risoluzioni, interrogazioni o interpellanze. Queste informazioni, eccetto quelle idonee a rivelare lo stato di salute, possono inoltre essere diffuse ai sensi del d.lg. n. 267/200 in ottemperanza al regime di pubblicita' degli atti e delle sedute dei consigli comunali, delle commissioni e degli altri organi comunali (art. 65, comma 5, d.lg. n. 196/2003). Le attivita' ricomprese in questo trattamento sono le attivita' di competenza degli Organi istituzionali (Sindaco, Giunta, Consiglio e commissioni consiliari) nonche' degli Uffici di gestione giuridica del personale dipendente, di Relazioni con il Pubblico.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 33 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 18.08.2000, n. 267 - Statuto e regolamento comunale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza degli Organi istituzionali: Sindaco, Giunta, Consiglio e commissioni consiliari nonche' degli Uffici di gestione giuridica del personale dipendente, di Relazioni con il Pubblico.
Nome archivio/Banca dati	- Scheda n. 33 - Sistema informativo relativo all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare lo stato di salute: anamnesi familiare - Dati idonei a rivelare la vita sessuale
Luoghi di	- In Italia

copia informatica per consultazione

custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 33 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: Altri servizi generali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 33 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonche' documentazione delle attivita' istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attivita' di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari ai sensi dell'art. 2-sexies, comma 2 lett. f) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (controllo, di indirizzo politico e di sindacato ispettivo e documentazione dell'attivita' istituzionale di organi pubblici)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 33 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): amministrazioni interessate o partecipi delle questioni oggetto dell'attivita' politica, di controllo e di sindacato ispettivo
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicita' dei lavori dei consigli comunali, delle commissioni e degli altri organi comunali (D.Lgs. n. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di	

copia informatica per consultazione

trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Amministratori - Enti locali - Revisori - Segretario comunale
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento:	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine

copia informatica per consultazione

termine ultimo per la cancellazione delle diverse categorie di dati	identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza

copia informatica per consultazione

	di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks

copia informatica per consultazione

indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare
  3 = alto = = e' **probabile** che la minaccia si possa verificare
  4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da

copia informatica per consultazione

un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la	

copia informatica per consultazione

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile	Soggetto individuato in base agli atti di organizzazione

copia informatica per consultazione

attuazione misure	

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo strategico ai sensi dell'art. 147-ter del D.Lgs. 267/2000
Istruttoria delle deliberazioni

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

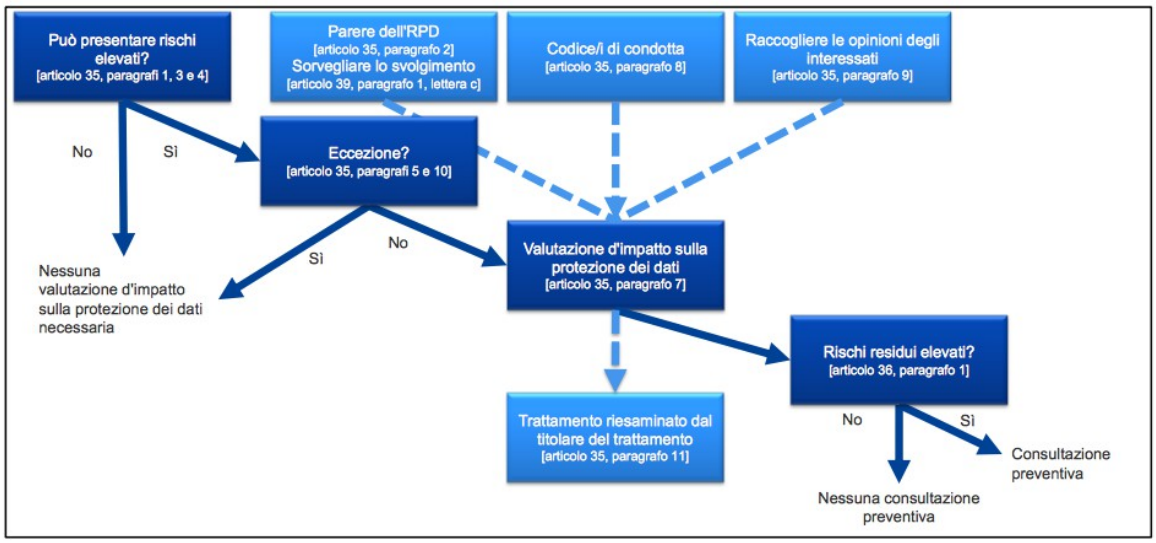
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

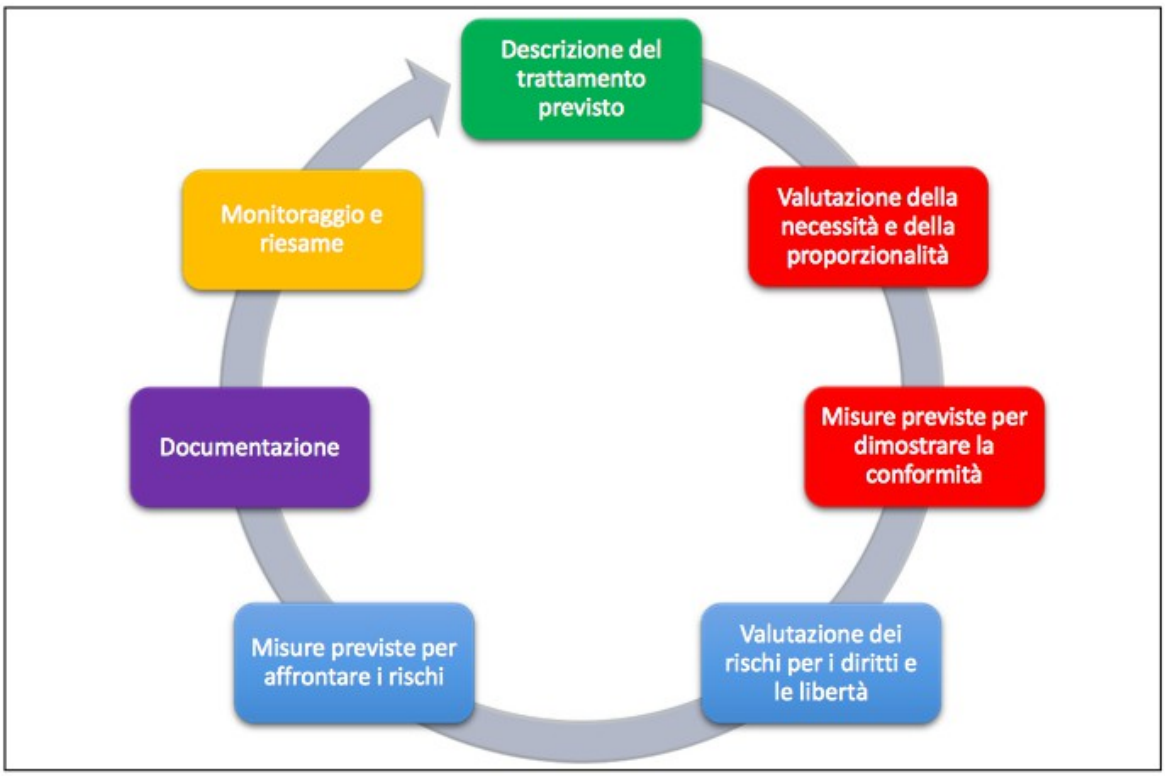
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 42 - I dati vengono acquisiti dagli interessati al momento del sopralluogo e dell'ispezione o verifica; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti o eventuali violazioni rispetto alle dichiarazioni acquisite. I dati sono registrati in archivi/ banche di dati gestite con modalita' elettroniche e su supporti cartacei tramite sistema informativo, controlli esterni, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 42 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art.

copia informatica per consultazione

	1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - D.Lg. n. 50/2016 - Reg. UE 679/2016 - DL. 24 novembre 1981 n. 689 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sui controlli interni
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 42 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 42 - Trattamento effettuato per attivita' di controllo, ispettive, comprese le attivita' di sopralluogo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 42 -Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di controllo, ispettive, comprese le attivita' di sopralluogo con la polizia locale)
Interesse legittimo	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in

copia informatica per consultazione

perseguito	forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: ***comunicazione***	- Scheda n. 42 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Autorita' giudiziaria, autorita' di pubblica sicurezza (per accertamenti di carattere giudiziario); b) al RUP e alla stazione appaltante (D.Lgs. n. 50/2016); c) alle autorita' amministrative di vigilanza (D.Lgs. n. 50/2016)
Categorie di trattamenti - particolari forme di elaborazione: ***diffusione***	N.R.
Categorie di trattamenti - particolari forme di elaborazione: ***trasferimento all'estero***	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Persone fisiche - Cittadini italiani - Persone giuridiche ed altri enti (comprende societa' di persone)

copia informatica per consultazione

	- Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli

copia informatica per consultazione

interessati o loro rappresentanti	interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Controllo successivo di regolarita' amministrativa e contabile ai sensi dell'art. 147-bis del D.Lgs. 267/2000
Controllo - Ispezione

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

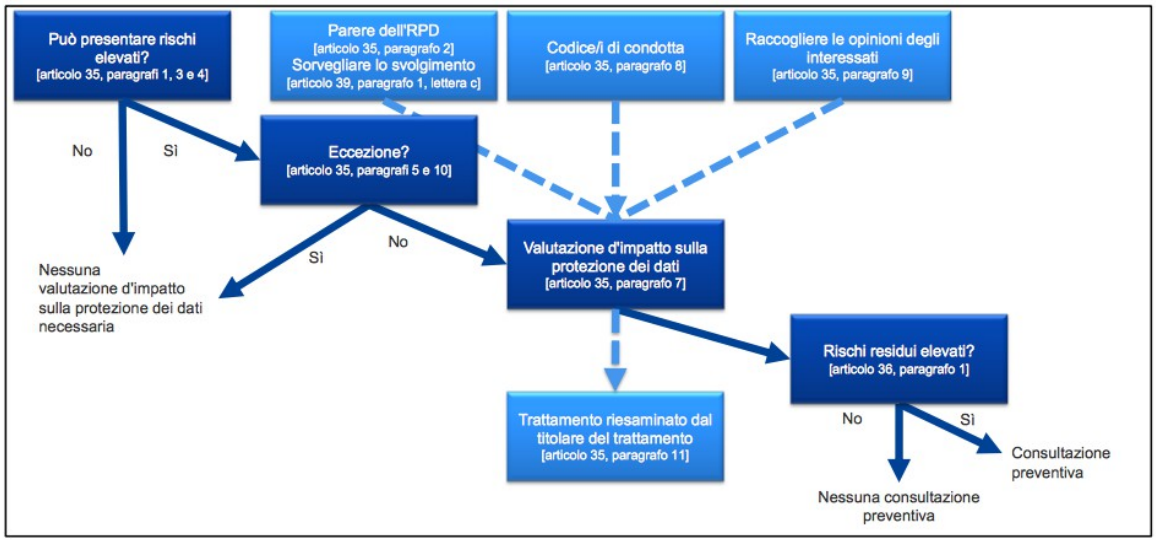
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

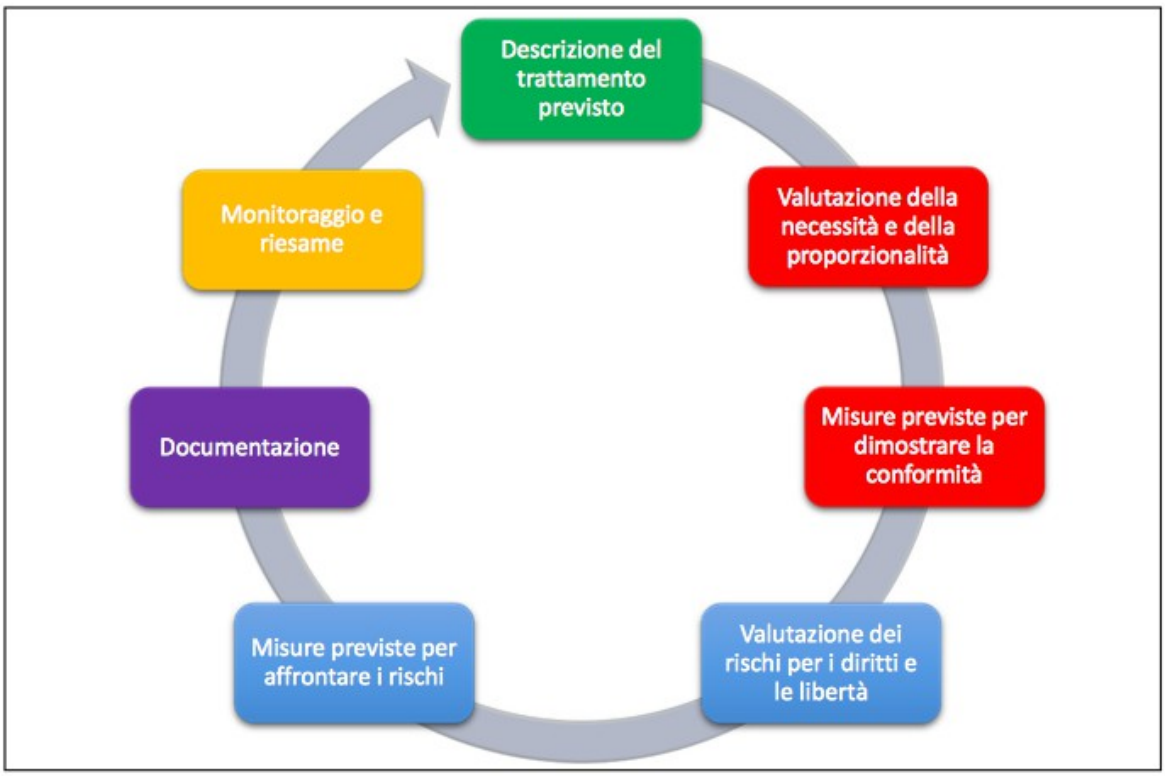
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 48 - Il trattamento ha per oggetto i dati relativi alla gestione del rischio di corruzione e illegalita'. I dati vengono raccolti d'ufficio, presso gli interessati e presso terzi che presentano esposti o segnalazioni. Comprende dati sensibili e giudiziari. Comporta la comunicazione a Procure (del Tribunale e Corte dei Conti) in caso di reato o danno erariale nonche' alle Autorita' di volta in volta competenti per le segnalazioni/ esposti (come, ad esempio, ANAC/AGCM). E' vietata la diffusione per essere il trattamento coperto dal segreto istruttorio salvo i casi previsti dalla L. 190/2012.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 48 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art.

copia informatica per consultazione

	1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - L. n. 179/2017 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sui controlli interni
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 48 - Sistema informativo relativo a segnalazioni illeciti, atti e documenti del sistema di gestione del rischio di corruzione e illegalita' - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 48 - Trattamento effettuato per finalita' di prevenzione del rischio di corruzione e illegalita'. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare

copia informatica per consultazione

Rilevanti finalita' di interesse pubblico	- Scheda n. 48 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 48 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): comunicazione a Procure del Tribunale e Corte dei Conti in caso di reato o danno erariale, nonche' alle Autorita' di volta in volta competenti per le segnalazioni/ esposti come, ad esempio, ANAC/AGCM (ai sensi dell'art. 331 c.p.p. e della L.190/2012)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del*	

copia informatica per consultazione

sito web	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Segnalanti - esponenti - Soggetti terzi rispetto ai segnalanti, i cui dati rilevano nella procedura
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)

copia informatica per consultazione

Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario,

copia informatica per consultazione

	aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati* (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

copia informatica per consultazione

	VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di

copia informatica per consultazione

	trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Molto alto

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici	

copia informatica per consultazione

	MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

copia informatica per consultazione

	- MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Segnalazione-Esposto
Segnalazioni di illecito

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

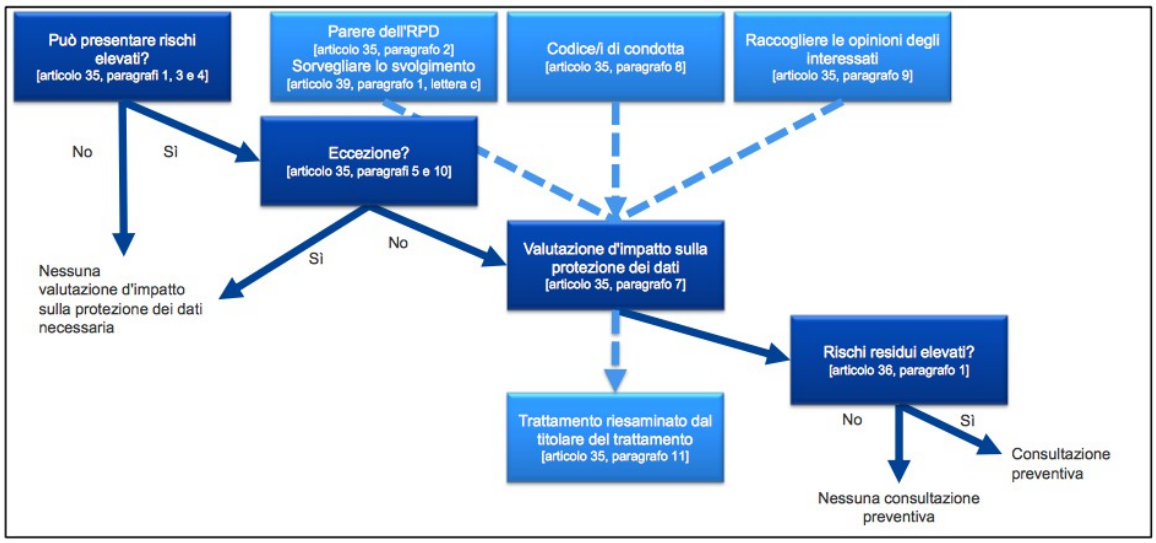
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

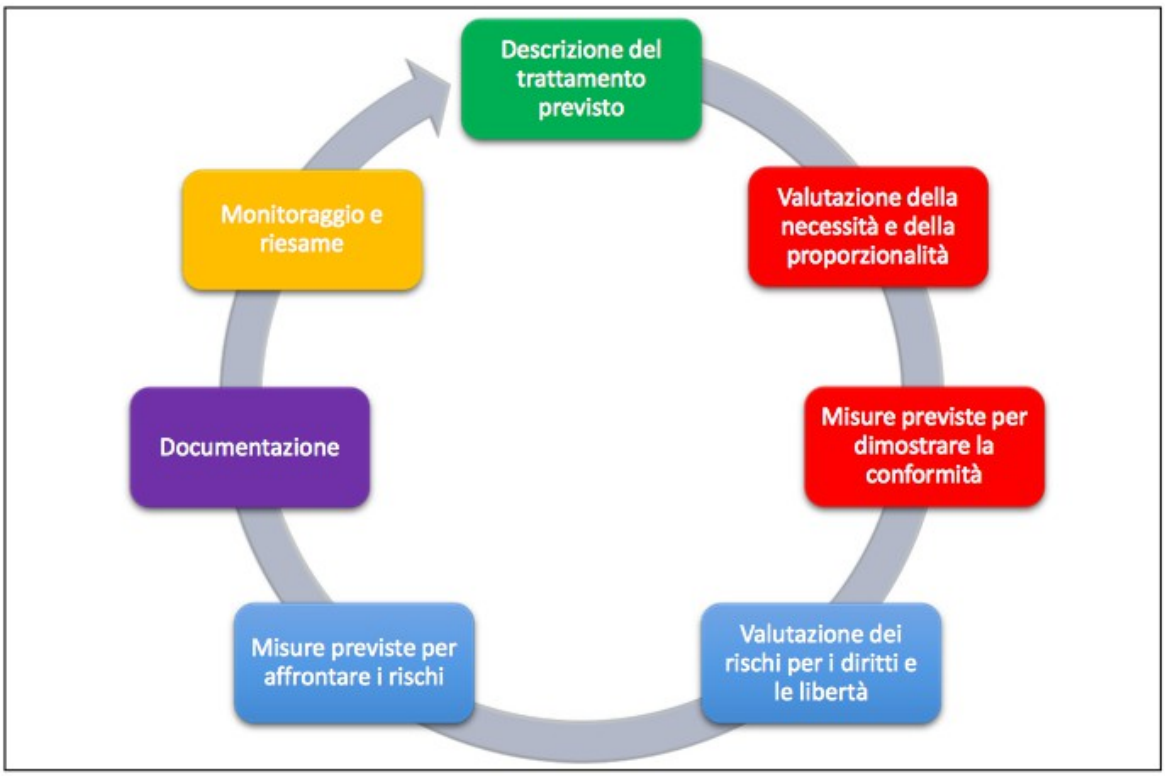
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 49 - I dati vengono raccolti per la conclusione di transazioni e per la gestione di lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento. Particolari forme di elaborazione tramite interconnessione e raffronto dati con altri soggetti pubblici o privati: amministrazioni certificanti ai sensi del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 49 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000

copia informatica per consultazione

	- D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo - Codice Civile - Codice procedura Civile
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 49 - Sistema informativo relativo a beni immobili, demaniali e patrimoniali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare la posizione di beni, strumenti, oggetti
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 49 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 49 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita'

copia informatica per consultazione

	direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita' di lasciti e transazioni nonche' donazioni e del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 49 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) altre amministrazioni e soggetti privati (ai sensi del Regolamento sulla disciplina dei contratti, del Regolamento di contabilita' e della normativa dagli stessi richiamata)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Persone fisiche - Persone giuridiche ed altri enti (comprende societa' di persone)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta

copia informatica per consultazione

	salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune

copia informatica per consultazione

	modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete

copia informatica per consultazione

	con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC

copia informatica per consultazione

	4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA	Alto

copia informatica per consultazione

PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a)

copia informatica per consultazione

	Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Autorizzazione al ricorso a transazioni e altri rimedi di risoluzione delle controversie alternativi a quelli giurisdizionali

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

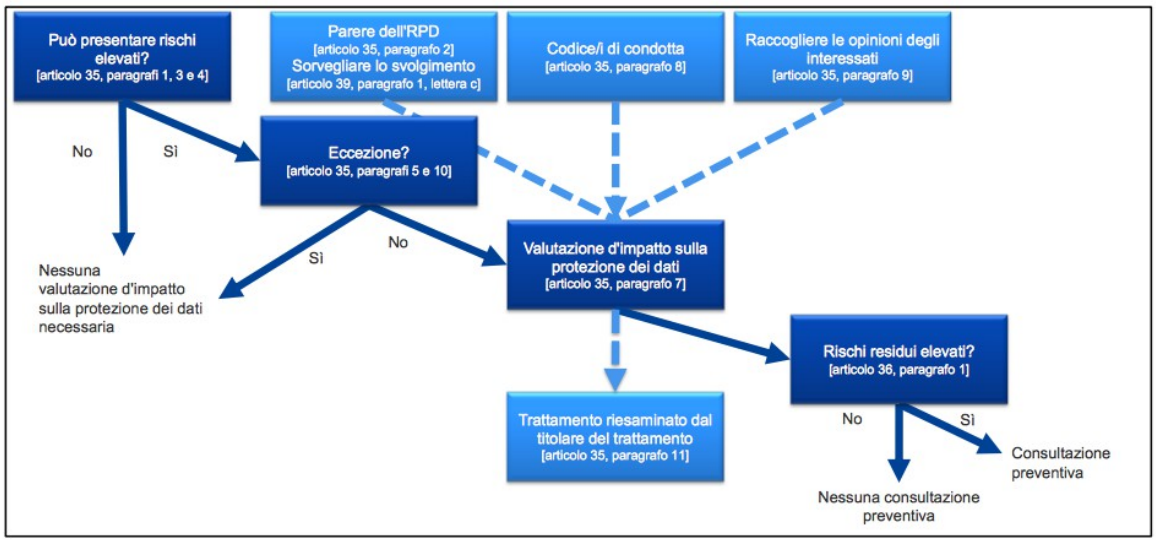
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

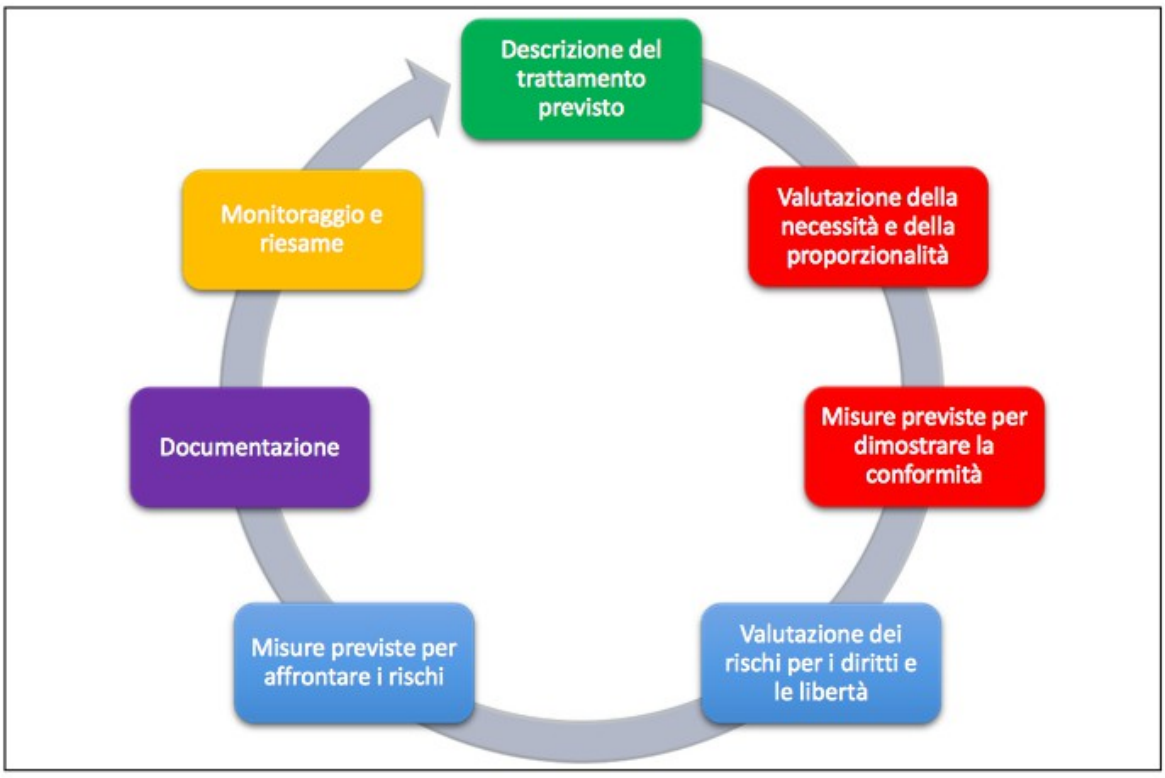
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Soggetto affidatario del servizio di gestione sito web istituzionale TINN srl Soggetto affidatario della fornitura servizio di firma digitale
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 50 - Il trattamento ha per oggetto i dati delle procedure di affidamento e dei contratti di appalto e di concessione delle amministrazioni aggiudicatrici e degli enti aggiudicatori per l'acquisizione di servizi, forniture, lavori e opere, nonche' i concorsi pubblici di progettazione e l'attivita' posta in essere in attuazione del D.Lgs. n. 50/2016. I dati vengono raccolti dai soggetti partecipanti alle procedure di affidamento e includono dati sensibili e giudiziari. Il trattamento implica, oltre alle ordinarie forme di elaborazione standardizzate (con mezzi elettronici e su supporto cartaceo), anche la comunicazione a terzi e, in particolare, alle Autorita' competenti a rilasciare le certificazioni sul possesso dei requisiti, nonche' la possibile diffusione mediante pubblicazione sul profilo del committente e sui siti web prescritti dalla normativa vigente in materia.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo - D.Lgs. 267/2000 T.U.E.L. - D.Lgs. 50/2016
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza trasversalmente, di tutti gli uffici che aggiudicano contratti inclusi nell'ambito di applicazione del D.Lgs. 50 n. 0/2016
Nome archivio/Banca dati	- Scheda n. 50 - Sistema informativo relativo ad appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati comuni, diversi dai dati particolari - Dati di accesso e di identificazione (user name, password, customer ID, altro) - Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili - Dati relativi al comportamento debitorio - Dati relativi all'affidabilita' o puntualita' nei pagamenti - Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati relativi all'adempimento di obbligazioni - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a

copia informatica per consultazione

	comportamenti illeciti o fraudolenti - Dati sensibili - Dati relativi all'affidabilita' nell'esecuzione dei contratti pubblici - Dati comuni identificativi - Indirizzo di posta elettronica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 50 - Trattamento effettuato per finalita' di adempimento di obblighi contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 50 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Altre amministrazioni ed enti pubblici - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi - Scheda n. 50 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Agenzia Entrate, Prefettura, Tribunale, Procura presso il Tribunale, Provincia e altri enti pubblici - INPS/INAIL/ANAC - , anche

copia informatica per consultazione

	attraverso la consultazione delle relative Banche dati, per i controlli sul possesso dei requisiti dichiarati in sede di procedura di affidamento; b) altri soggetti partecipanti alla procedura di affidamento; c) consulenti e soggetti, pubblici o privati, che effettuano servizi di committenza ausiliaria; d) avvocati incaricati dell'eventuale contenzioso (ai sensi del D.Lgs. n. 50/2016 e della regolazione attuativa)
Categorie di trattamenti - particolari forme di elaborazione: ***diffusione***	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione sul sito web, in "Amministratrazione trasparente" in attuazione di obblighi di pubblicazione di cui al D. Lgs. n. 33/2013 - Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: ***trasferimento all'estero***	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Utenti (anche potenziali) - Concorrenti alle procedure di affidamento di contratti pubblici - Soggetti terzi rispetto ai concorrenti, i cui dati rilevano nella procedura di affidamento
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il

copia informatica per consultazione

	ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013

copia informatica per consultazione

Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle

copia informatica per consultazione

	specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI **Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati** (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA INCIDENTI: crimeware (malware che mirano a ottenere il controllo dei sistemi) - CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento -TRATTAMENTI ELETTRONICI: utilizzo di parole chiave non adeguate - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	
STIMA (XxY)	

copia informatica per consultazione

DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e	

copia informatica per consultazione

	implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI

copia informatica per consultazione

sicurezza: Organizzative	ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a)

copia informatica per consultazione

	Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Documentare la conformita' al RGPD	- La conformita' giuridica al regolamento generale sulla protezione dei dati e' provata dal documento di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dal documento di DPIA - La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Gare ad evidenza pubblica di concessione di beni e servizi
Liquidazioni acconti o rata di saldo e omologa del certificato di regolare esecuzione per contratti pubblici di lavori, servizi e forniture in economia
Convenzioni con associazioni di volontariato
Proroga contratto in scadenza
Adesione convenzioni CONSIP o del Soggetto Aggregatore di riferimento
Affidamento appalto di servizi e forniture di importo superiore alle soglie di cui all'art. 14, D.Lgs. 36/2023 attraverso il sistema della procedura aperta
Affidamento appalto di servizi e forniture di importo pari o superiore a 140.000 euro e inferiore alle soglie di cui all'articolo 14, D.Lgs. 36/2023 mediante il sistema della procedura negoziata
Affidamento mediante procedura aperta (o ristretta) di lavori, servizi, forniture
Affidamento diretto di lavori, servizi o forniture
Proposta di aggiudicazione in base al prezzo
Proposta di aggiudicazione in base all'OEPV
Pulizia degli immobili e degli impianti di proprieta' dell'ente

22

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

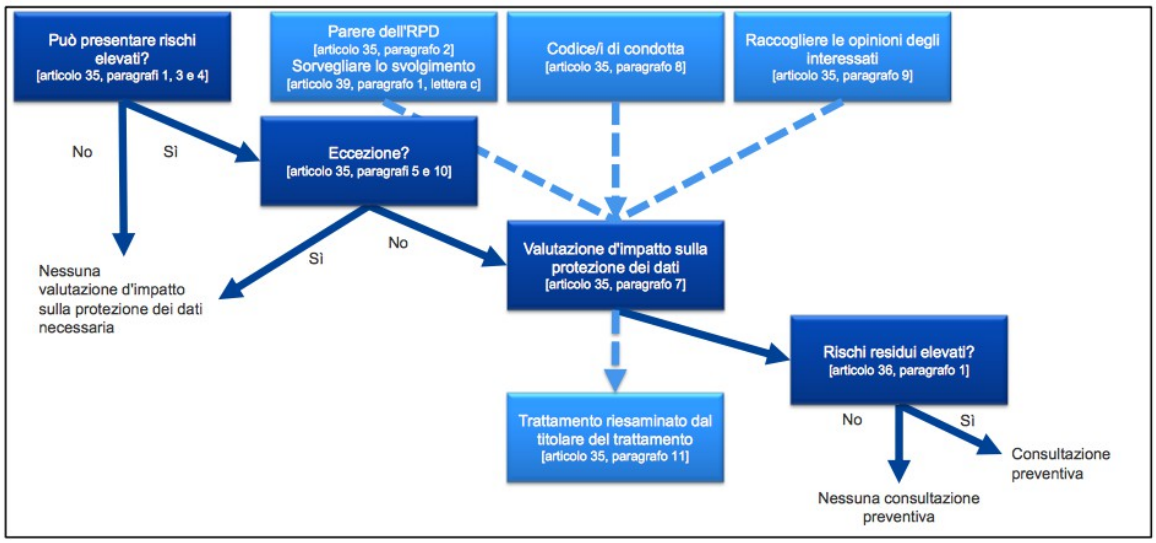
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

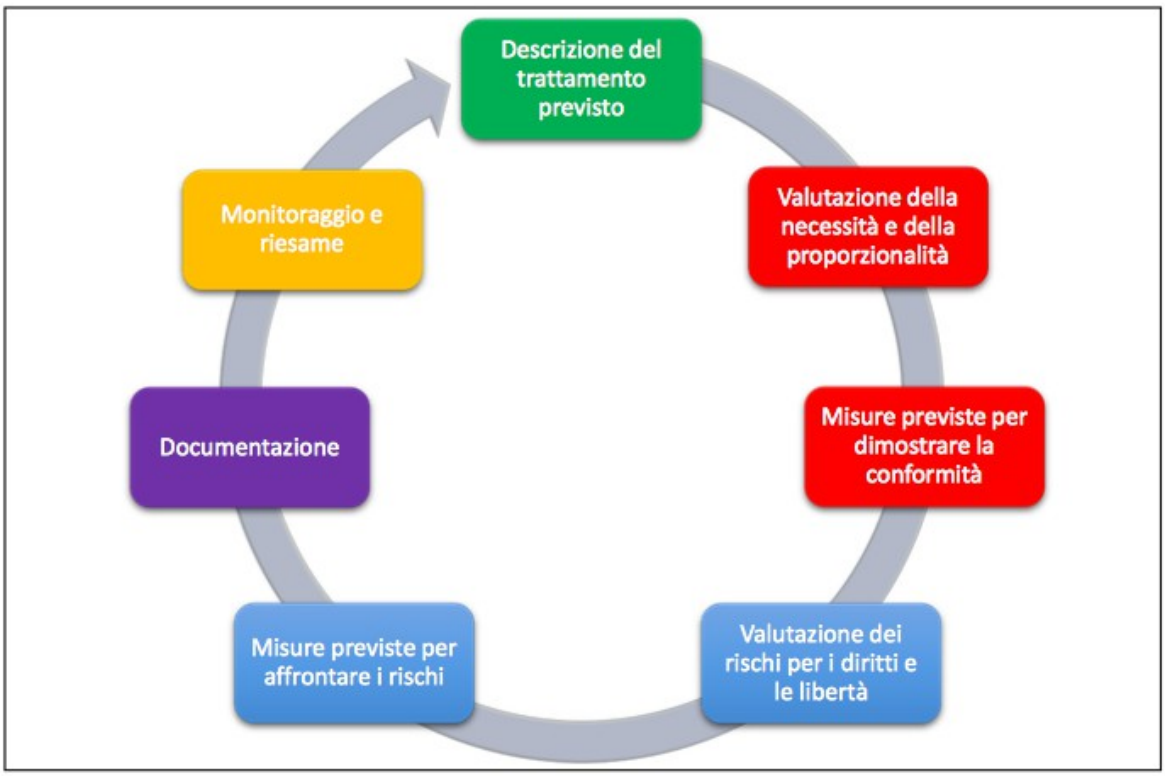
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 51 - I dati personali trattati nei procedimenti di accesso documentale, civico semplice e di accesso civico generalizzato vengono raccolti sia presso l'interessato che presso terzi. Il trattamento puo' includere anche dati vulnerabili. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo. In relazione ad alcuni trattamenti (quali ad esempio, l'accesso civico semplice e l'accesso civico generalizzato) vengono effettuate anche operazioni particolari di comunicazione, interconnessione e raffronti di dati (con specificazione ed indicazione della base normativa): con altri trattamenti o banche dati dello stesso ente.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 51 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 97/2016 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sull'accesso
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 51 - Sistema informativo relativo ad accesso e trasparenza - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 51 - Trattamento effettuato per finalita' di trasparenza dell'attivita' amministrativa. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare

copia informatica per consultazione

Rilevanti finalita' di interesse pubblico	- Scheda n. 51 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: conferimento di onorificenze e ricompense, riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali ai sensi dell'art. 2-sexies, comma 2 lett. n) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento al riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' di rilascio e revoca di autorizzazioni o abilitazioni, di concessione di patrocini, patronati e premi di rappresentanza, di adesione a comitati d'onore e di ammissione a cerimonie ed incontri istituzionali
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 51 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): controinteressati ai sensi della L. 241/1990 e D.Lgs. 33/2013
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite*	

copia informatica per consultazione

un sito web-nome del dominio del sito web	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E. - Amministratori
Categorie di destinatari	- Soggetti privati - Soggetti pubblici - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o

copia informatica per consultazione

	storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere

copia informatica per consultazione

	realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza

copia informatica per consultazione

	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli	Alto

copia informatica per consultazione

interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

copia informatica per consultazione

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza:	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica	

copia informatica per consultazione

tecniche logistiche	- MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non

copia informatica per consultazione

	autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare

copia informatica per consultazione

	regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**

copia informatica per consultazione

art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Accesso civico semplice concernente dati, documenti e informazioni soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013
Accesso civico generalizzato concernente dati e documenti ulteriori a quelli soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013
Registro degli accessi

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

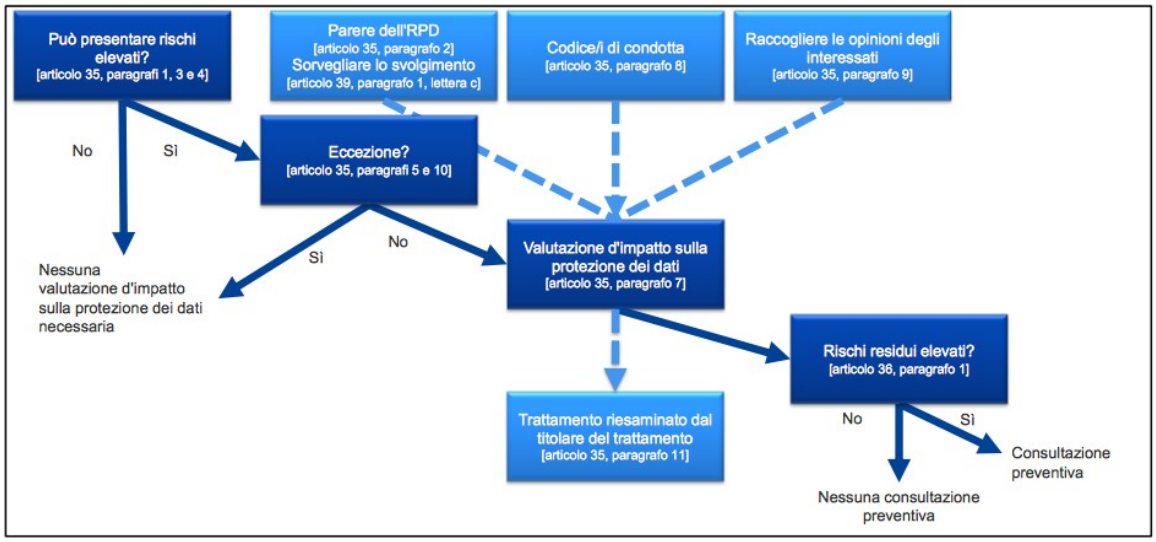
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

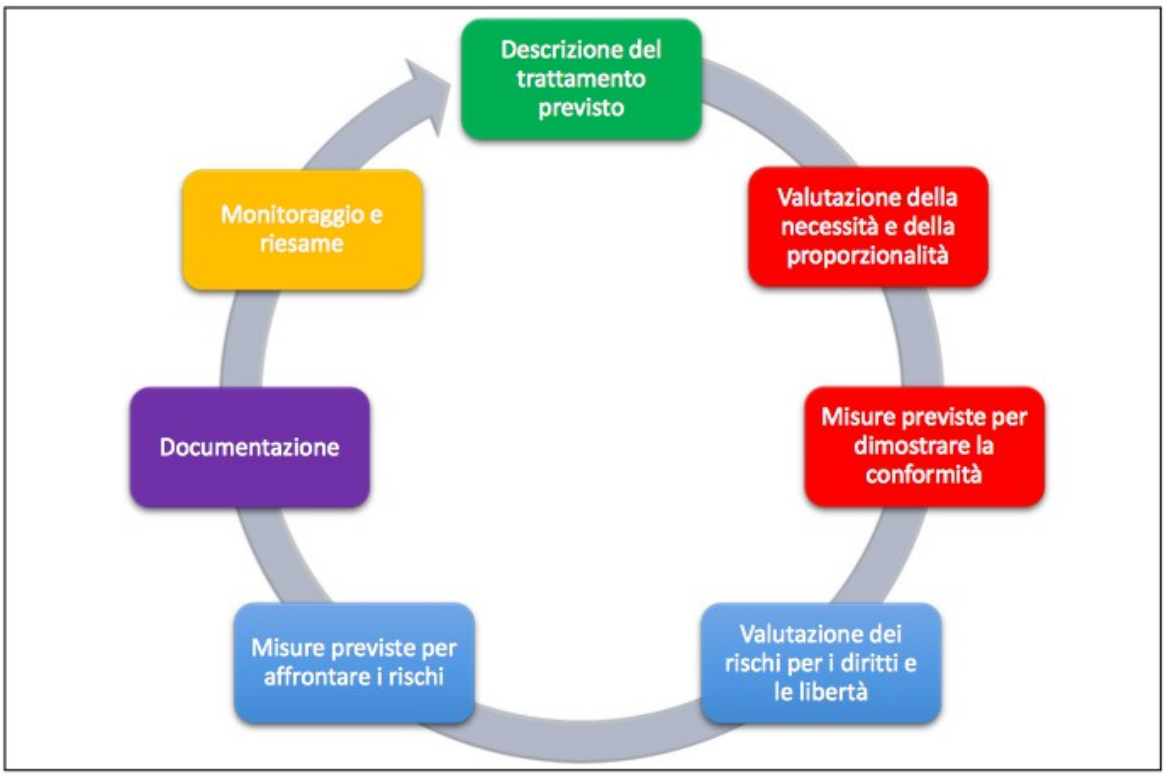
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 59 - I dati vengono nella gestione della rete informatica, dell'hardware e dei server, in relazione a dati personali in particolare dei dipendenti pubblici che utilizzano gli strumenti e degli utenti esterni che accedono alla rete.
Il trattamento puo' includere anche dati comuni e sensibili. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici, tramite sistema informativo, assistenza informatica, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n.114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Fonte normativa	- Scheda n. 59 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 59 - Base di dati: sistema informativo, assistenza informatica, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di accesso e di identificazione (user name, password, customer ID, altro)
Luoghi di custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 59 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 59 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico,inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed

copia informatica per consultazione

	ispettive nei confronti di altri soggetti)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Utenti (anche potenziali)

copia informatica per consultazione

Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione

copia informatica per consultazione

Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Gestione S.I. e rete: Creazione caselle di posta elettronica

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO	Servizio Segreteria Sindaco e Relazioni Esterne

TRATTAMENTO	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

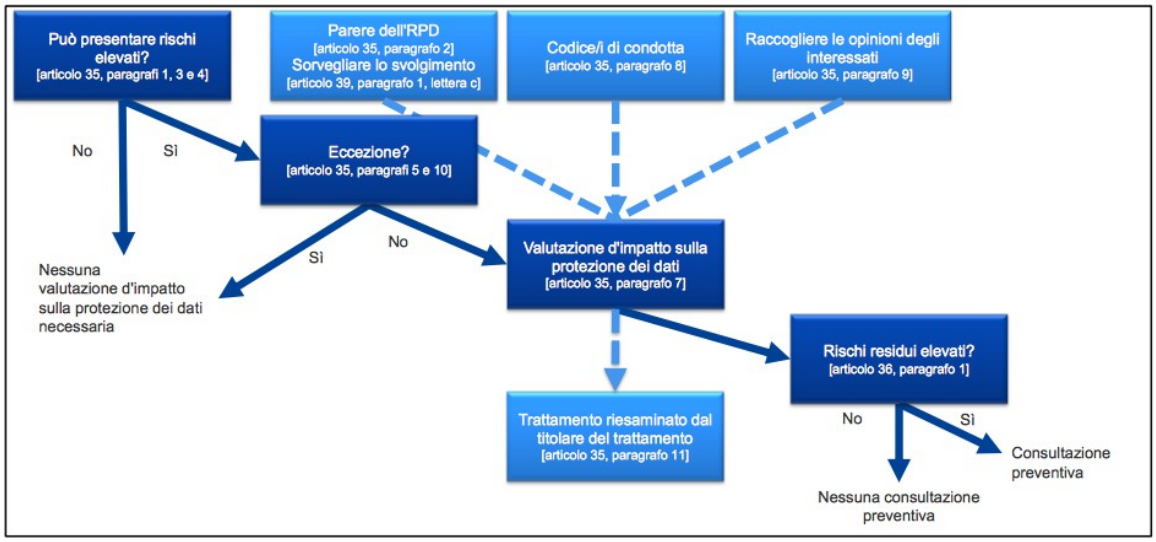
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

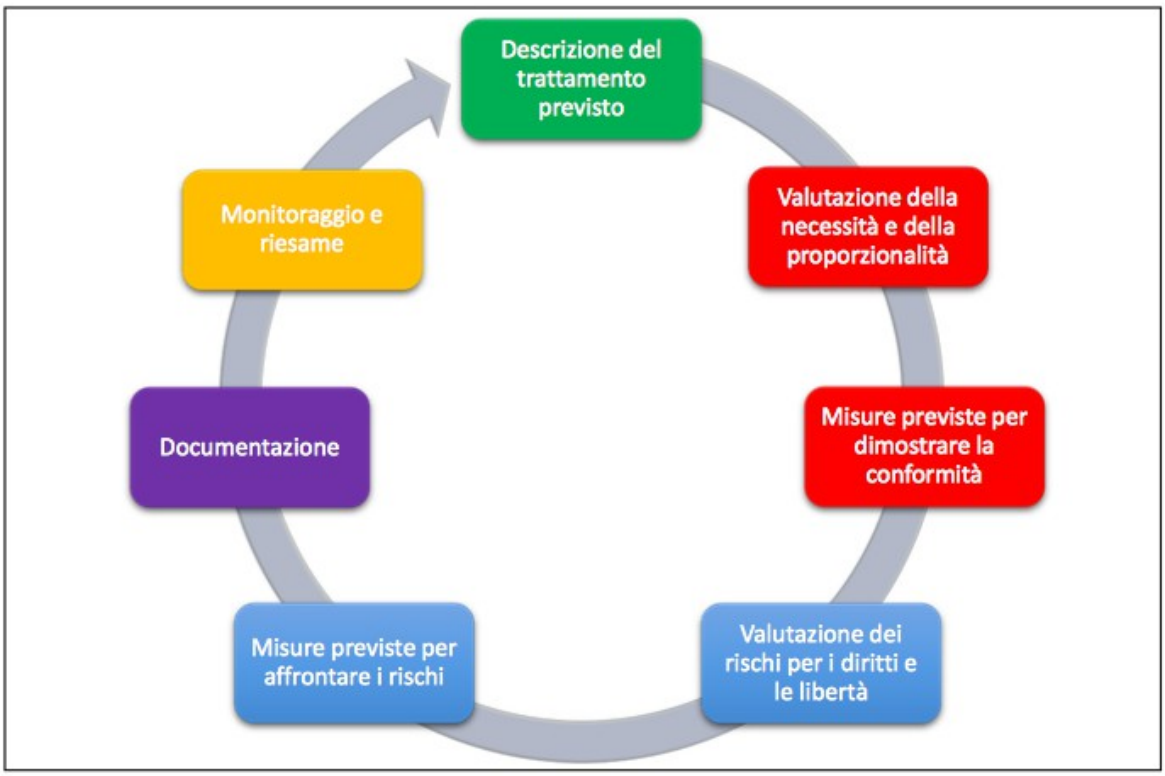
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE
SERVIZIO: denominazione e punti di contatto	Servizio Segreteria Sindaco e Relazioni Esterne
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	Gestione associata archivi storici - Comune Marciana Gestione associata archivi storici - Comune di Portoferraio Gestione associata archivi storici - Comune di Rio Gestione associata archivi storici - Comune di Porto Azzurro Gestione associata archivi storici - Comune di Capoliveri Gestione associata archivi storici - Comune di Marciana Marina
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano Dott.ssa Galli M. Cristina dott.ssa Gargiulo Michela dott.ssa Peria Gloria dott.ssa Segnini Marina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 61 - I dati vengono raccolti dall'Ufficio Segreteria e protocollo sia presso l'ente, sia presso terzi, sia presso gli interessati. Il trattamento (che include anche dati vulnerabili e sensibili) e' effettuato per rilevanti finalita' di interesse pubblico relative verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo tramite sistema informativo, protocollo interno, raccolta pratiche, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n.114/2014.

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 61 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 61 - Sistema informativo relativo al protocollo interno e raccolta pratiche - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 61 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare

copia informatica per consultazione

Rilevanti finalita' di interesse pubblico	- Scheda n. 61 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: volgimento delle funzioni di controllo, indirizzo politico,inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Cittadini italiani - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o

copia informatica per consultazione

	storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere

copia informatica per consultazione

	realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza

copia informatica per consultazione

	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli	Alto

copia informatica per consultazione

interessati)	
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

copia informatica per consultazione

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza:	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica	

copia informatica per consultazione

tecniche logistiche	- MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non

copia informatica per consultazione

	autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante

copia informatica per consultazione

	- MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Stampa giornaliera ed annuale del registro di protocollo informatico
Gestione dell'archivio storico

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

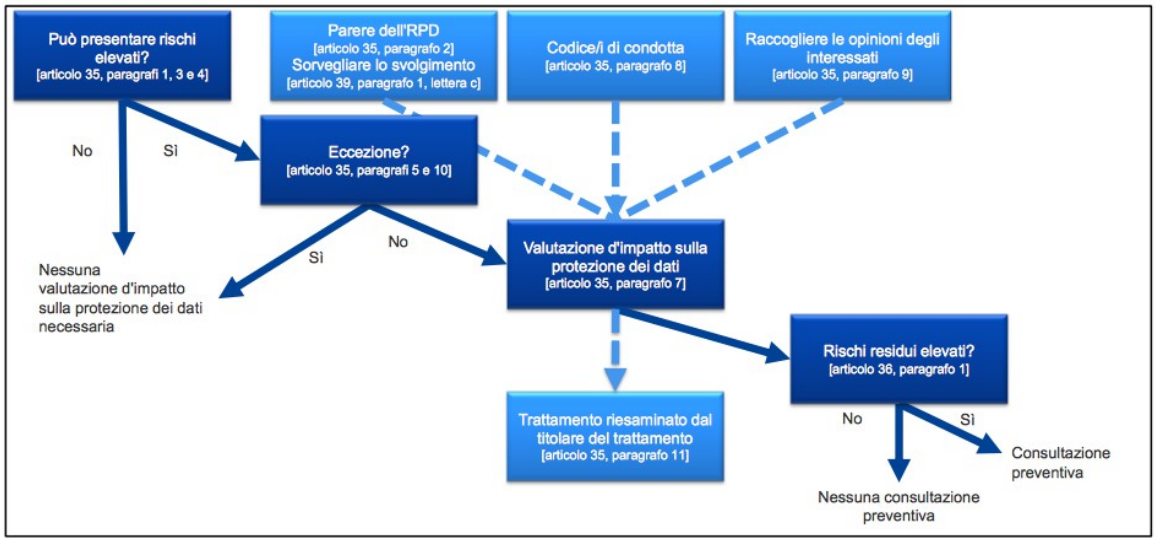
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

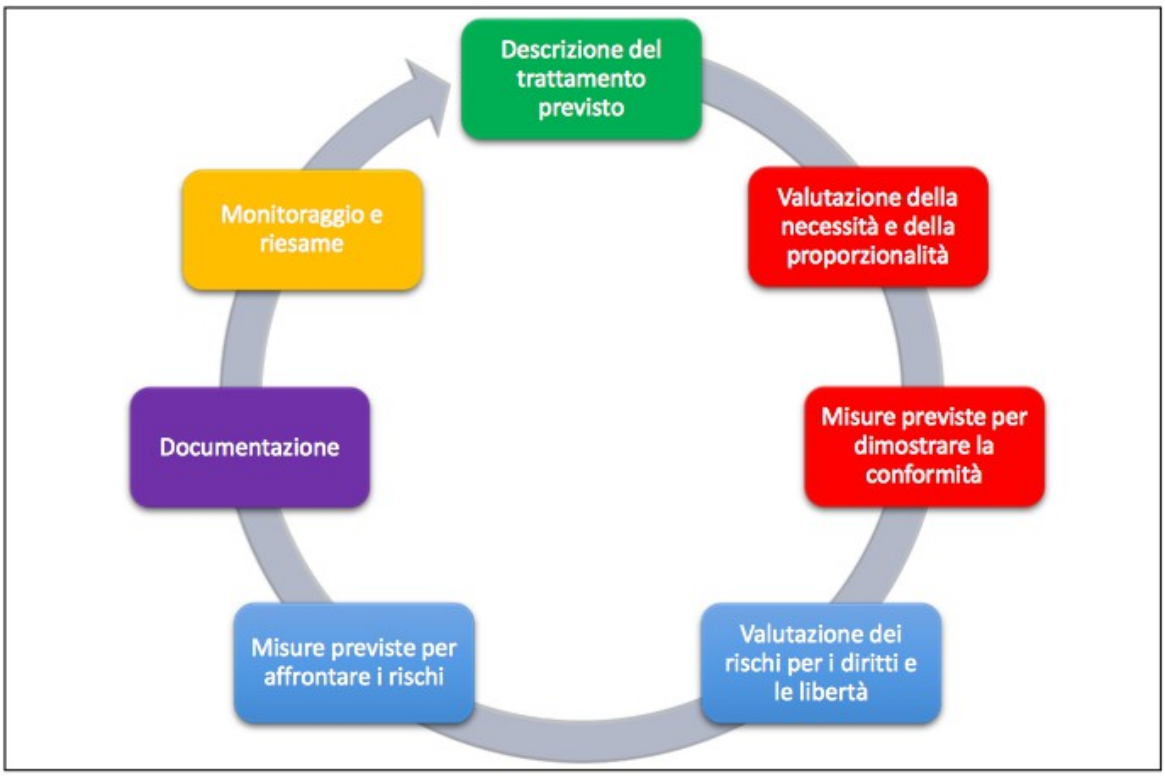
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Cooperativa Sociale Arca G. Di Vittorio Societa' Cooperativa Sociale Onlus Cooperativa Sociale C.I.S.S.E. Soc. Coop. Soc. "Europa Servizi"
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 10 - I dati vengono forniti direttamente dagli interessati, i quali presentano apposita domanda al Comune ovvero da terzi (Polizia municipale e Forze di polizia; INPS, ASL, azienda ospedaliera, IPAB, medici di base; scuola dell'infanzia e Istituti di istruzione). Il Comune comunica le informazioni alle ASL, alle Aziende ospedaliere, alle Regioni, nonche' alle cooperative sociali ed ad altri enti che effettuano i singoli interventi di sostegno e assistenza. I dati vengono trasmessi anche all'Autorita' giudiziaria per l'eventuale adozione un provvedimento di interdizione, di inabilitazione o la nomina di un amministratore di sostegno.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 10 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000

copia informatica per consultazione

	- D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 3.05.2000, n. 130 - L. 8.11.2000, n. 328 - Art. 406 c.c. - regolamenti comunali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 10 - Sistema informativo relativo alla domiciliarita', comprensivi i servizi e assistenza economica - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 10 - Trattamento effettuato per finalita' di diritti sociali, politiche sociali e famiglia: Interventi per la disabilita'. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 10 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci ai sensi dell'art. 2-sexies, comma 2 lett. s) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (interventi di carattere socio-assistenziale, anche di rilievo sanitario, in favore di soggetti bisognosi o non

copia informatica per consultazione

	autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 10 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) ASL, Aziende ospedaliere e Regioni (per comunicare l'evoluzione della situazione, i controlli e le verifiche periodiche, il monitoraggio dell'attivita'); b) cooperative sociali e ad altri enti (cui vengono affidate le attivita' di assistenza)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di*	

copia informatica per consultazione

ubicazione del/i server	
Categorie di interessati	- Persone disabili - Assistiti - Soggetti con limitata capacita' di intendere e volere
Categorie di destinatari	- Soggetti privati - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto

copia informatica per consultazione

Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Molto alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - livello dell'impatto, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Servizio assistenza domiciliare minori

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

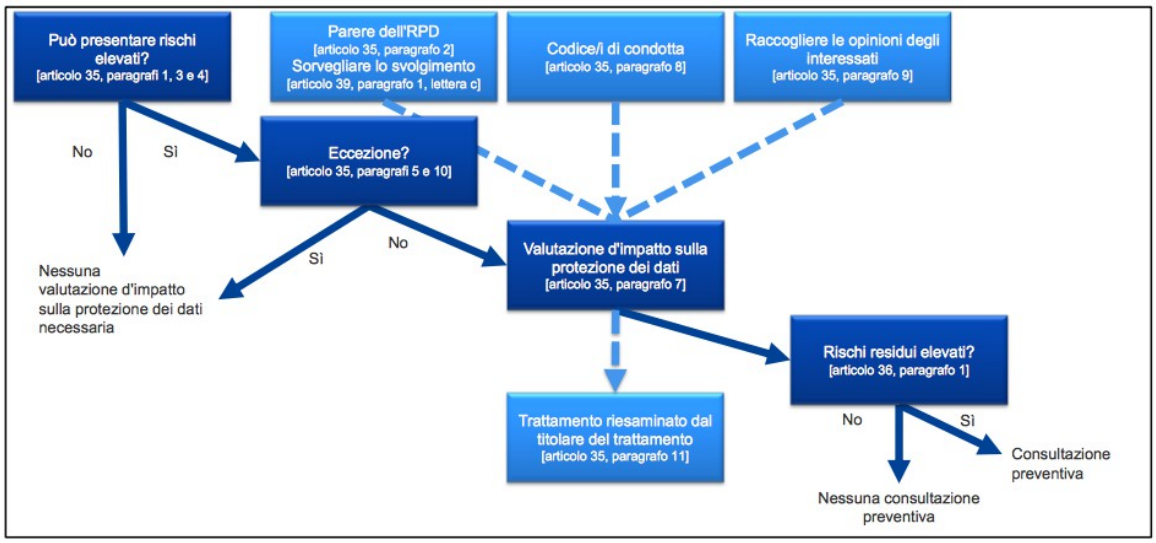
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

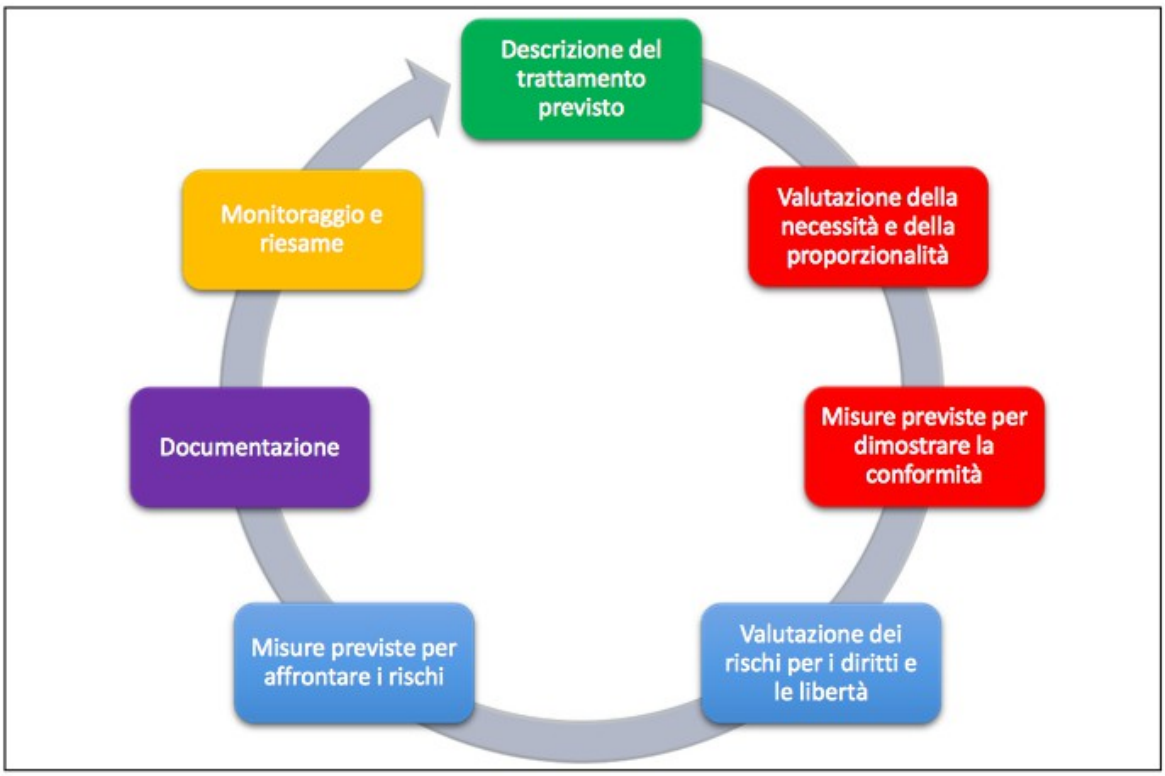
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 12 - I dati vengono forniti da terzi (medico di base, ASL, Polizia municipale e Forze di polizia, Autorita' giudiziaria) o dall'interessato, che presenta un'apposita istanza, o d'ufficio (dalle ASL e/o Aziende ospedaliere per valutare lo stato di non autosufficienza psico-fisica e per reperire le informazioni, di carattere sanitario, relative all'interessato), attraverso l'operato degli assistenti sociali: la domanda deve essere corredata della documentazione (anche sanitaria) necessaria. I dati possono essere comunicati alle ASL competenti e all'Autorita' giudiziaria, al fine di avviare le procedure necessarie per il ricovero del soggetto interdetto o inabilitato presso gli istituti di cura. I dati vengono altresi' comunicati ai gestori delle case di riposo ed alla direzione delle strutture residenziali, al fine di garantire l'erogazione del servizio in favore del soggetto ricoverato. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Fonte normativa	- Scheda n. 12 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (art. 403) - D.P.R. 24.07.1977, n. 616 - L. 8.11.2000, n. 328 - Leggi regionali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 12 - Sistema informativo relativo ad attivita' relative alla concessione di benefici economici e agli interventi di sostegno per la problematica abitativa, compresi i contributi sul canone di locazione non agevolato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare lo stato di salute: anamnesi familiare
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 12 - Trattamento effettuato per finalita' relative a: interventi, anche di carattere sanitario, in favore di soggetti bisognosi o non autosufficienti o incapaci. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del

copia informatica per consultazione

	servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 12 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci ai sensi dell'art. 2-sexies, comma 2 lett. s) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (interventi, anche di carattere sanitario, in favore di soggetti bisognosi o non autosufficienti o incapaci)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 12 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Autorita' giudiziaria (per avviare le procedure di ricovero relative ai soggetti interdetti o inabilitati); b) ASL ed Aziende ospedaliere, (per trasmettere le informazioni, di carattere sanitario, relative all'interessato); c) gestori delle case di riposo, alla direzione delle strutture residenziali (per l'erogazione del servizio)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del*	

copia informatica per consultazione

sito web	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Utenti (anche potenziali) - Pazienti, degenti o disabili
Categorie di destinatari	- Autorita' giudiziaria - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)

copia informatica per consultazione

Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario,

copia informatica per consultazione

	aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati* (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

copia informatica per consultazione

	VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di

copia informatica per consultazione

	trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici	

copia informatica per consultazione

	MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach

copia informatica per consultazione

	- MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Concessione integrazione rette case di riposo
Servizio RSA e riabilitazione
Servizi per disabili
Servizio ricovero minori in struttura

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

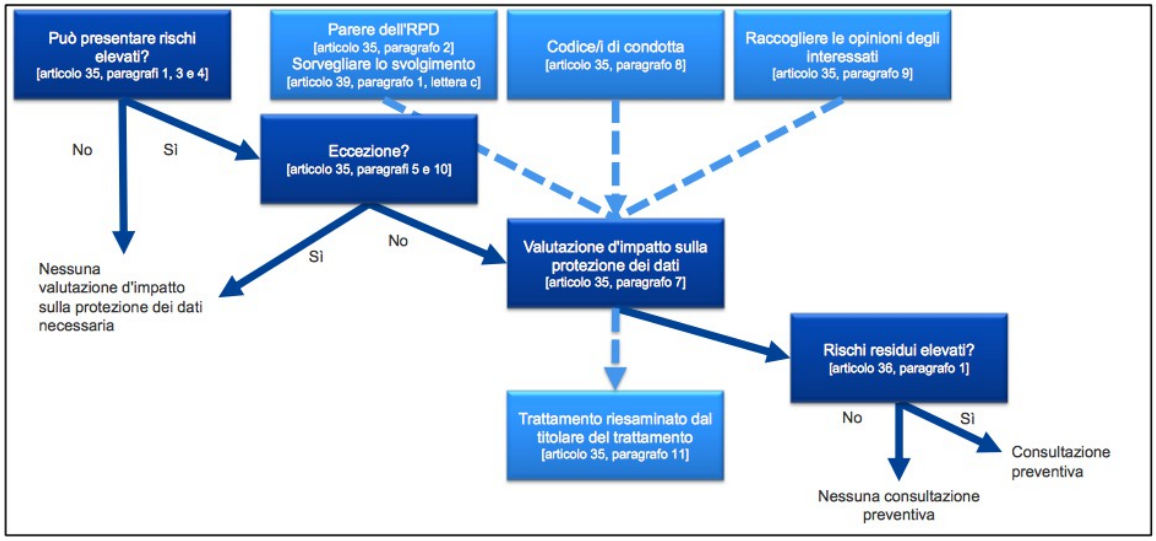
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

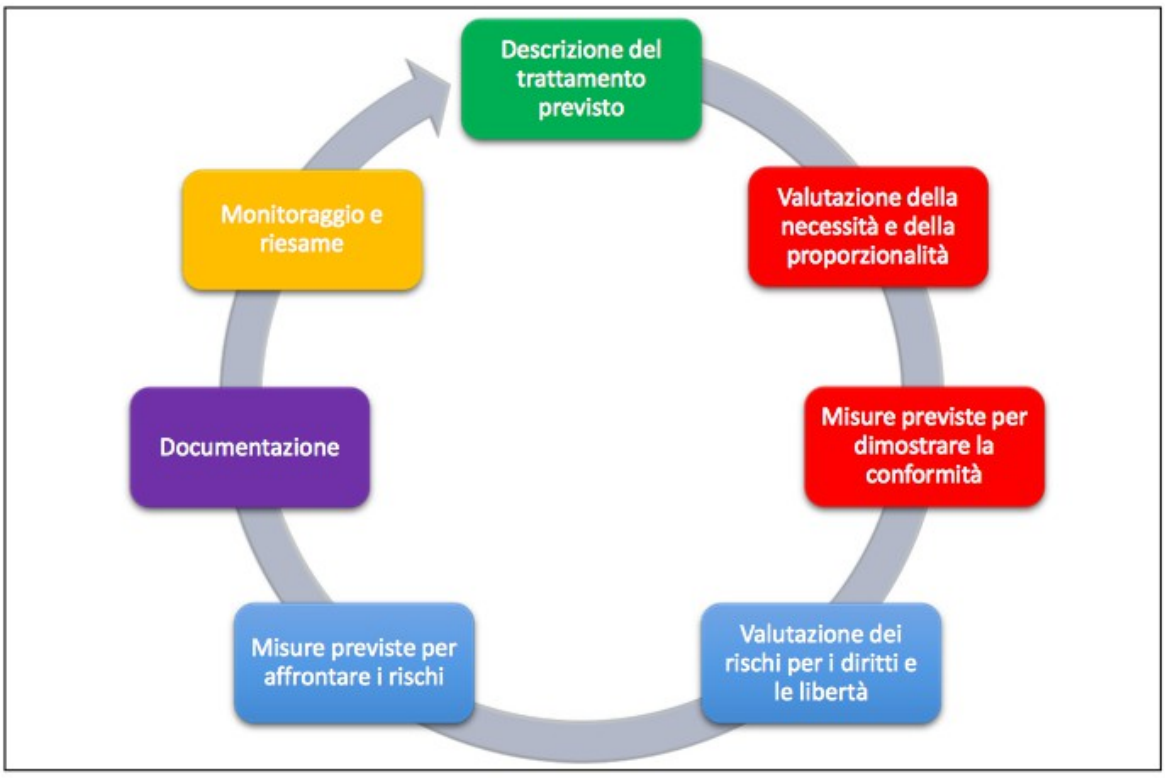
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	ANCI - SGATE
Responsabile trattamento: denominazione e punti di contatto	Cooperativa Sociale Arca Azienda USL Toscana Nord Ovest
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 14 - I dati vengono forniti dall'interessato, previa presentazione dell'istanza per accedere al contributo e/o al ricovero, ovvero da terzi (ASL o tutore, per predisporre una relazione di valutazione dello stato di non autosufficienza psico-fisica relativa all'interessato). Le informazioni sulla salute sono comunicate unicamente all'istituto che presso il quale viene effettuato il ricovero, in particolare viene comunicata l'ammissione del beneficiario, il grado di invalidita' e le particolari patologie dell'interessato, al fine di garantire un'assistenza mirata. Le eventuali convinzioni religiose e filosofiche possono invece rilevare ai fini dell'erogazione di particolari regimi alimentari. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 14 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 5.12.1992, n. 104 - D.Lgs. 31.03.1998, n. 112 e relative disposizioni di attuazione - D.Lgs. 18.08.2000, n. 267 - leggi regionali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 14 - Sistema informativo relativo a concessione di contributi, sussidi e benefici - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare lo stato di salute: anamnesi familiare
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 14 - Trattamento effettuato per finalita' relative ad attivita' socio-assistenziali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla

copia informatica per consultazione

	legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 14 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci ai sensi dell'art. 2-sexies, comma 2 lett. s) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' socio-assistenziali)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 14 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Istituto che fornisce la prestazione (ai sensi della l. n. 328/2000) - Altre amministrazioni ed enti pubblici - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Utenti (anche potenziali)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta

copia informatica per consultazione

	salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune

copia informatica per consultazione

	modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati* (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi

copia informatica per consultazione

	di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5

copia informatica per consultazione

	(CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti

copia informatica per consultazione

	- CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto	

copia informatica per consultazione

	con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita

copia informatica per consultazione

	l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di

copia informatica per consultazione

	ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Concessione contributi economici
Concessione contributi per badanti
Concessione Carta per ottenere agevolazioni presso gli esercizi commerciali
Contrassegni
Concessione buono casa
Concessione buono elettricista
Servizio di controllo I.S.E.E. per prestazioni sociali agevolate
Servizio di gestione tariffe e rette

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 15 - Servizi sociali - Trattamento di dati relativi all'attivita' di gestione dell'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

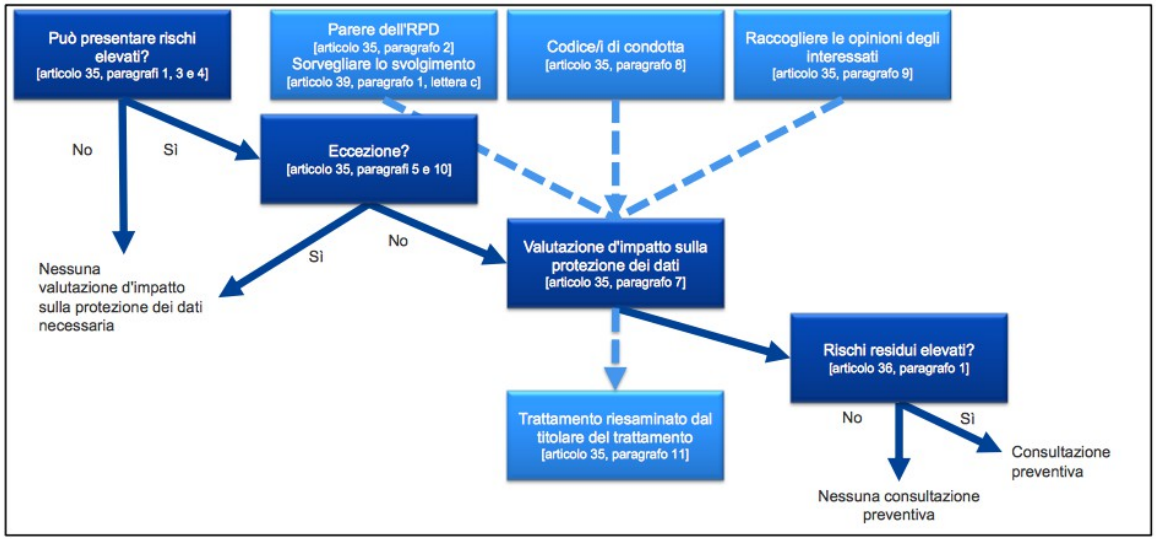
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

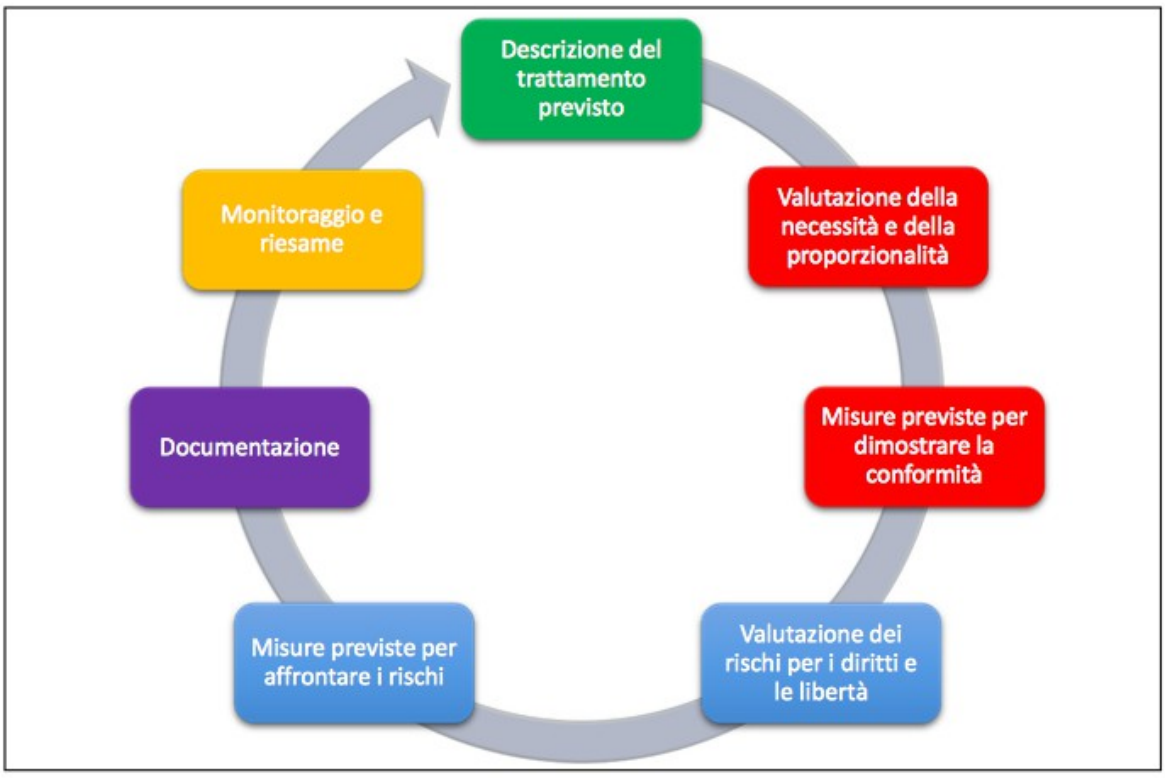
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	G. Di Vittorio Societa' Cooperativa Sociale Onlus Cooperativa Sociale C.I.S.S.E. Soc. Coop. Soc. "Europa Servizi"
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 15 - I dati vengono forniti dall'interessato, che presenta un'apposita istanza per la fruizione dei servizi, corredata della necessaria documentazione anche sanitaria. Le informazioni vengono quindi comunicate all'ente, all' impresa o all'associazione che provvede all'erogazione del servizio, nonche' agli istituti scolastici per l'integrazione social, l'istruzione e l'erogazione del servizio in favore del soggetto portatore di handicap. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 15 - Principi dell'ordinamento dell'Unione europea e normativa europea

copia informatica per consultazione

	pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 28.08.1997, n. 285 - L. 8.11.2000, n. 328 - L. 5.02.1992, n. 104 - leggi regionali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 15 - Sistema informativo relativo all'attivita' relativa all'integrazione sociale ed all'istruzione di soggetti che versano in condizioni di disagio sociale e psico-sociale (centro diurno, centro socio educativo, ludoteca, ecc.) - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 15 - Trattamento effettuato per finalita' di adempimenti previdenziali - assistenziali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 15 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: tutela sociale della maternita' ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili ai sensi

copia informatica per consultazione

	dell'art. 2-sexies, comma 2 lett. aa) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (interventi di sostegno psico-sociale e di formazione in favore di giovani o altri soggetti che versano in condizioni di disagio sociale, economico o familiare; integrazione sociale e istruzione del portatore di handicap)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 15 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Enti, imprese o associazioni in convenzione, istituti scolastici (per attuare le misure necessarie a garantire l'inserimento del soggetto bisognoso e l'erogazione del servizio)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i*	

copia informatica per consultazione

server	
Categorie di interessati	- Utenti (anche potenziali) - Assistiti
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Servizi assistenziali e socio-sanitari per anziani

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

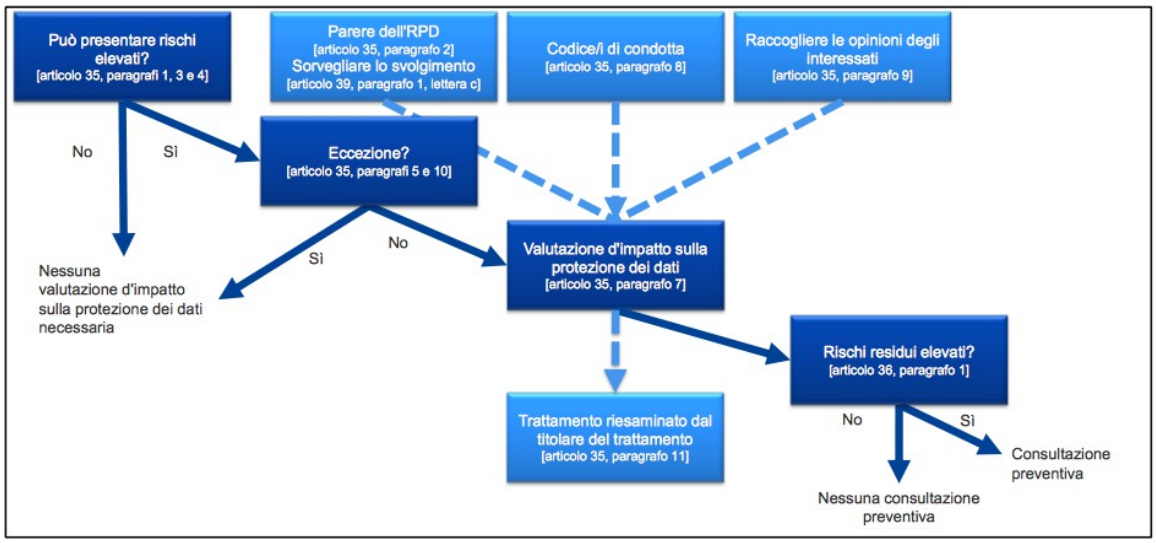
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

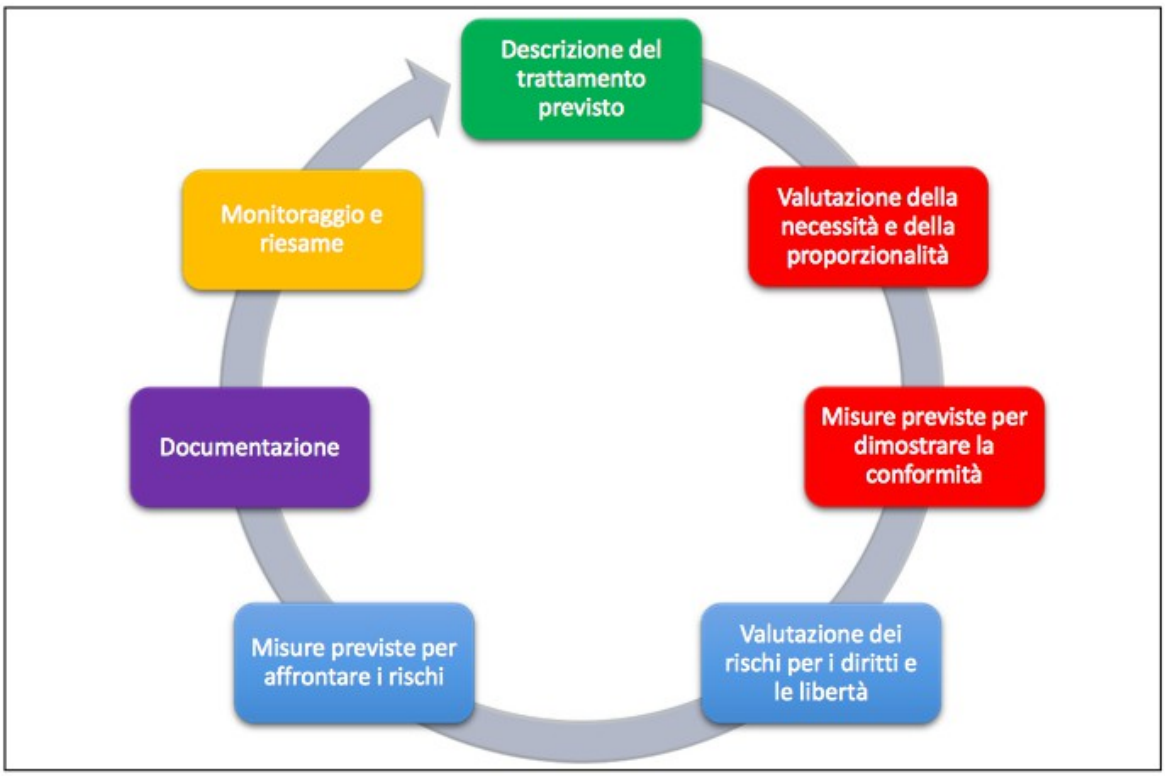
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	G. Di Vittorio Societa' Cooperativa Sociale Onlus Cooperativa Sociale C.I.S.S.E.
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 16 - I dati vengono forniti dall'interessato, ovvero dai suoi tutori o dai suoi curatori, i quali presentano un'apposita istanza corredata della necessaria documentazione sanitaria. Alcune informazioni possono essere acquisite anche dalla ASL in quanto i comuni, d'intesa con le aziende unita' sanitarie locali, possono predisporre su richiesta dell'interessato, un progetto individuale di integrazione e sostegno sociale. I dati vengono comunicati all'ente, all' impresa o all'associazione che effettua il servizio di trasporto. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 16 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni

copia informatica per consultazione

	(LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 5.02.1992, n. 104 - L. 8.11.2000, n. 328 - leggi regionali - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo - D.Lgs. 50/2016 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo - L. 104/1992 - Legge quadro per l'assistenza, integrazione sociale e diritti delle persone handicappate - Legge regionale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016
Nome archivio/Banca dati	- Scheda n. 16 - Sistema informativo relativo ad assistenza diretta e indiretta, benefici economici - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse

copia informatica per consultazione

	- Dati idonei a rilevare lo stato di salute: terapie in corso
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 16 - Trattamento effettuato per finalita' di adempimenti previdenziali - assistenziali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 16 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: tutela sociale della maternita' ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili ai sensi dell'art. 2-sexies, comma 2 lett. aa) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 16 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): enti, imprese o associazioni convenzionati che gestiscono il servizio di trasporto (per garantire l'erogazione del servizio)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di	

copia informatica per consultazione

trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Utenti (anche potenziali) - Assistiti
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza

copia informatica per consultazione

	di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks

copia informatica per consultazione

indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare
  3 = alto = = e' **probabile** che la minaccia si possa verificare
  4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da

copia informatica per consultazione

un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la	

copia informatica per consultazione

	sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile	Soggetto individuato in base agli atti di organizzazione

copia informatica per consultazione

attuazione misure	

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Servizio di trasporto anziani
Servizio trasporto extraurbano minori e disabili
Servizio trasporto urbano minori e disabili

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

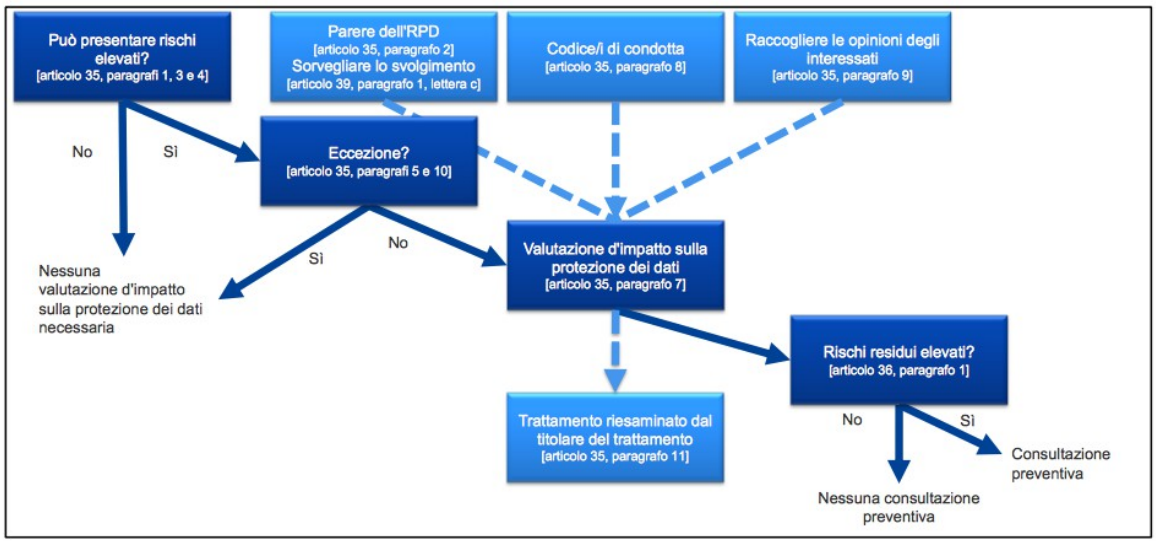
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

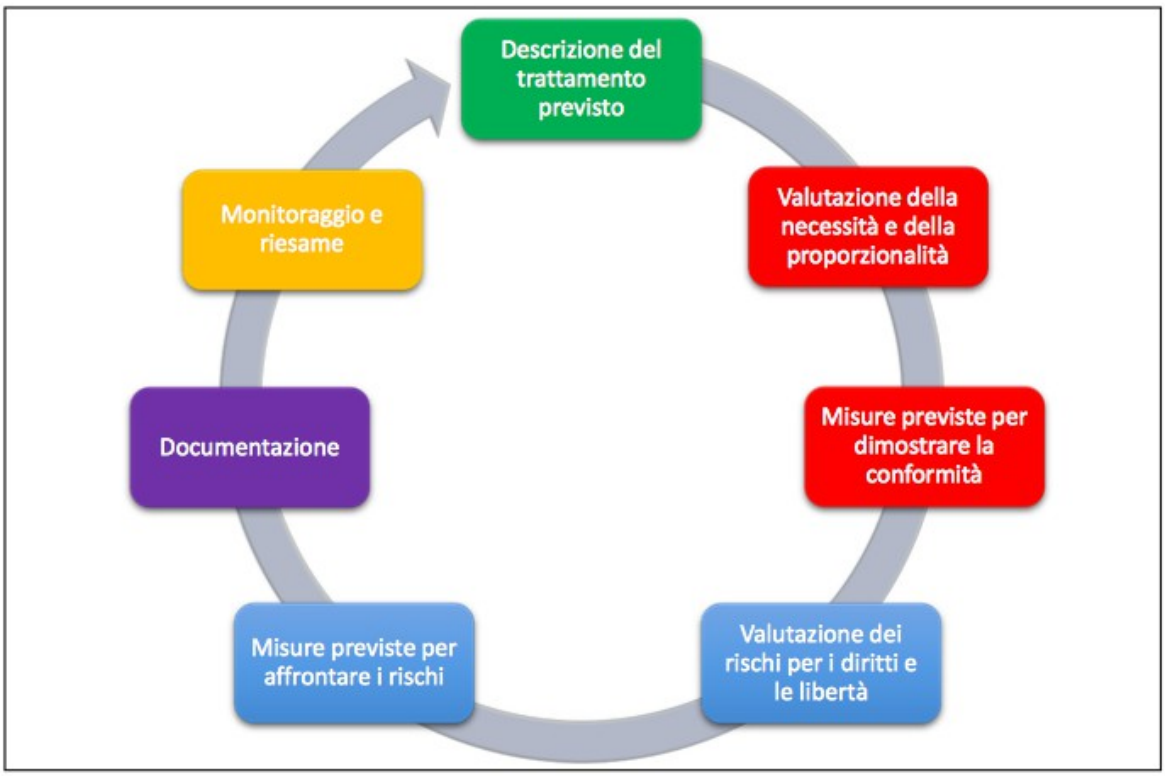
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 18 - Gli esiti dell'indagine, relativa allo stato di abbandono o di adattabilita' del minore, svolta dal Comune o dalla ASL, sono comunicati al Tribunale dei minori e, in caso di affidamento, al giudice tutelare, nonche' alle regioni al fine di procedere all'aggiornamento della banca dati dei minori adottabili (D.M. n. 91/2004). I dati cosi' raccolti confluiscono, quindi, nel provvedimento emanato dall'Autorita' giudiziaria. Inoltre, nell'ambito della ricerca della famiglia affidataria, possono essere valutati anche specifici precedenti giudiziari, nonche' le convinzioni di carattere religioso. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 18 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art.

copia informatica per consultazione

	1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (artt. 400 - 413) - D.P.R. 24.07.1977, n. 616 - L. 4.05.1983, n. 184 - L. 8.11.2000, n. 328 - L. 28.3.2001, n. 149 (art. 40) - Leggi regionali - regolamenti comunali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016
Nome archivio/Banca dati	- Scheda n. 18 - Sistema informativo relativo ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare lo stato di salute: anamnesi familiare
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 18 - Trattamento effettuato per finalita' relative a: assistenza nei confronti di minori, anche in relazione a vicende giudiziarie; vigilanza per affidamenti temporanei e indagini psico-sociali relative a provvedimenti di adozione anche internazionale. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 18 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci ai sensi dell'art. 2-sexies, comma 2, lett. s),

copia informatica per consultazione

	D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (assistenza nei confronti di minori, anche in relazione a vicende giudiziarie; vigilanza per affidamenti temporanei e indagini psico-sociali relative a provvedimenti di adozione anche internazionale)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 18 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Autorita' giudiziaria (Procura della Repubblica presso il Tribunale dei minori e Tribunale dei minori per ottenere l'assenso al procedimento); b) Regioni (per aggiornare la banca dati minori dichiarati adottabili)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-*	

copia informatica per consultazione

Paese/i di ubicazione del/i server	
Categorie di interessati	- Assistiti
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento:	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa

copia informatica per consultazione

modalita' di cessazione dei dati	comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati

copia informatica per consultazione

	- Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Procedure correlate alla nomina amministratore di sostegno, interdizione o inabilitazione (su richiesta dell'autorita' giudiziaria)
Gestione degli alloggi pubblici
Servizi per minori e famiglie
Servizi per adulti in difficolta'

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

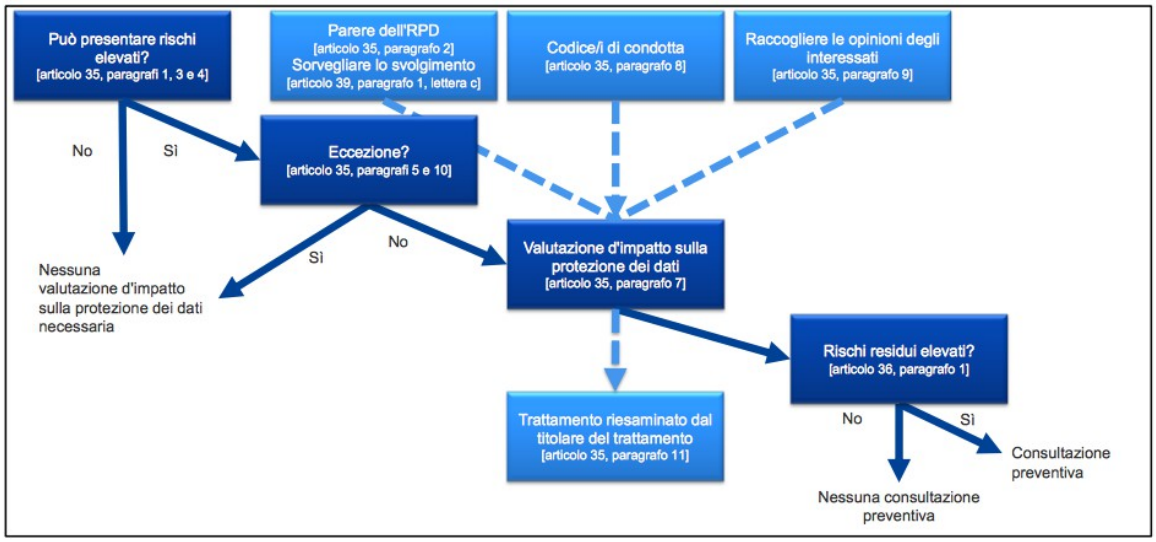
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

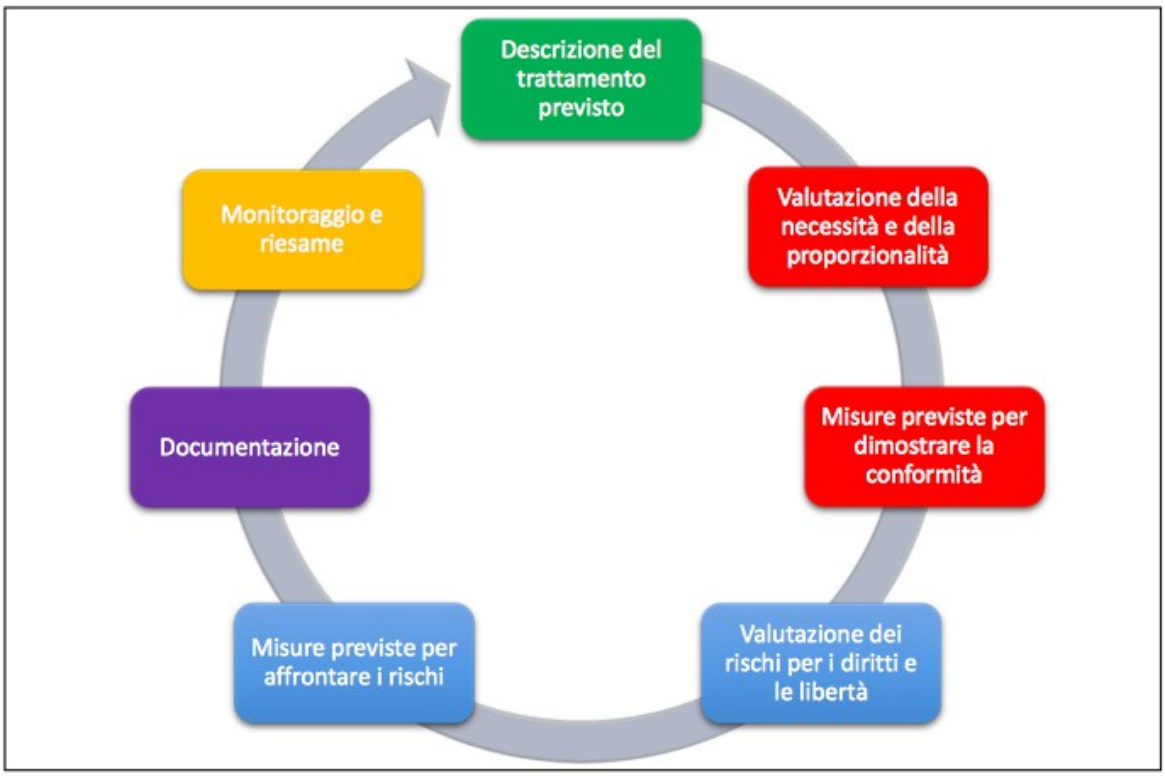
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 22 - Formazione degli allievi disabili: le certificazioni mediche d'invalidita' vengono fornite dagli interessati per organizzare i corsi di formazione professionale o scolastica, ovvero per l'inserimento lavorativo dei disabili. Servizio per gli adolescenti in difficolta' : i dati relativi ai minori sottoposti a procedimenti penali, civili e amministrativi vengono forniti dal Tribunale per i minorenni, al fine di elaborare un progetto educativo scolastico/lavorativo coordinato con i Servizi della giustizia minorile e il suddetto Tribunale. Scuole civiche: i dati sanitari sugli alunni disabili vengono forniti dalle famiglie alle scuole civiche per elaborare un progetto educativo integrato da parte degli organi collegiali delle scuole stesse. I dati sulla religione degli alunni sono forniti dalle famiglie per giustificare eventuali assenze dalle lezioni.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 22 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni

copia informatica per consultazione

	(LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.P.R. 24.07.1977, n. 616 - D.Lgs. 31.03.1998, n. 112 (art. 139) - Leggi regionali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 22 - Sistema informativo relativo a diritto allo studio e servizi - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare lo stato di salute: patologie attuali
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 22 - Trattamento effettuato per finalita' relative a: istruzione e formazione in ambito scolastico, superiore o universitario. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 22 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: istruzione e formazione in ambito scolastico, professionale, superiore o universitario ai sensi dell'art. 2-sexies, comma 2, lett. bb), D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una

copia informatica per consultazione

	delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 22 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): gestori esterni del servizio di trasporto scolastico - Altre amministrazioni ed enti pubblici - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ai soggetti interconnessi
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Utenti (anche potenziali)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT

copia informatica per consultazione

	(amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n.

copia informatica per consultazione

approvati	62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

copia informatica per consultazione

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

copia informatica per consultazione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA'	Alto

copia informatica per consultazione

E GRAVITA' (rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Servizio centro ricreativo estivo - CRE

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

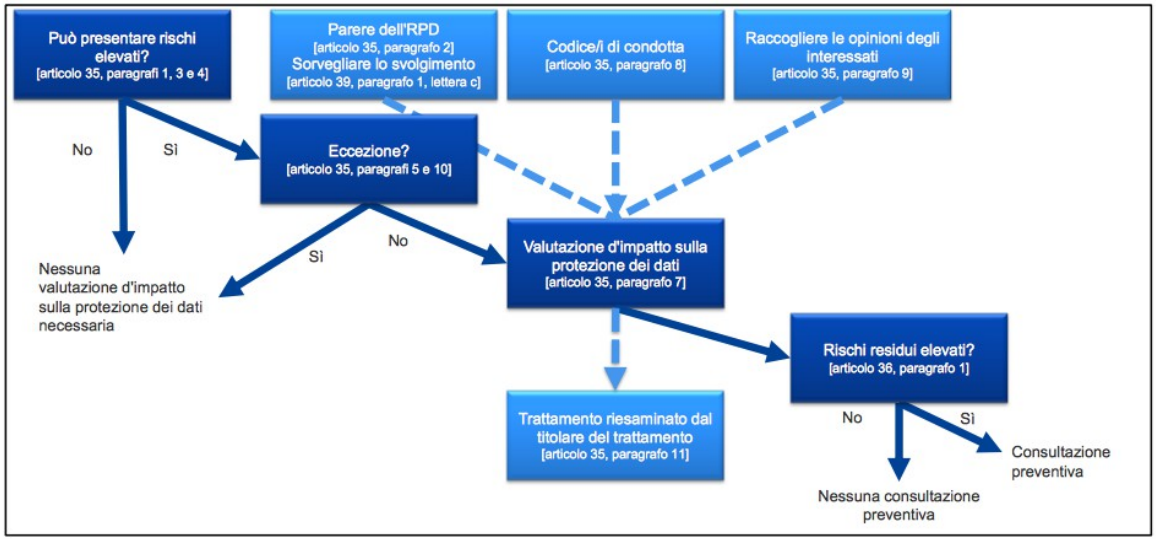
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

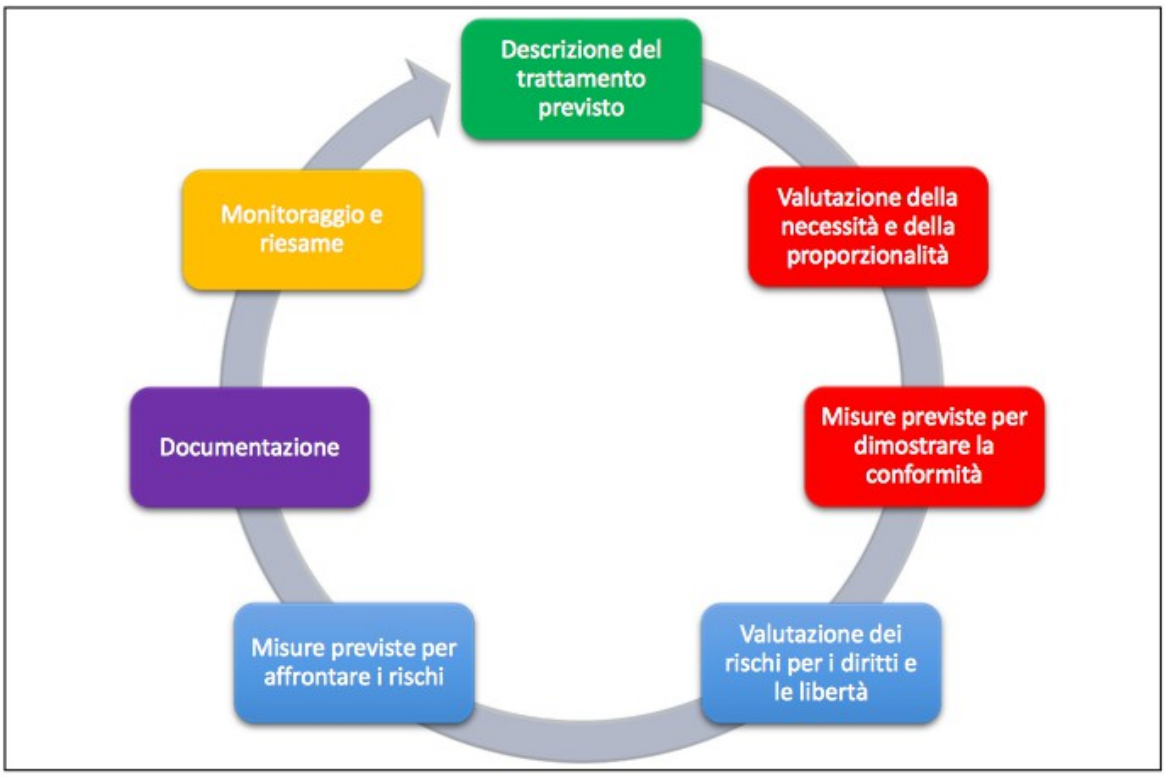
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 37 - I dati vengono raccolti presso gli interessati i quali possono richiedere, per particolari iniziative, il patrocinio e/o l'erogazione di un contributo economico e/o la collaborazione dell'Amministrazione Comunale. Al fine di valutare eventuali cause ostative all'erogazione di un contributo, viene acquisita la posizione debitoria con una dichiarazione sostitutiva ai sensi degli artt. 46 e 47 del D.P.R. 445/2000. Altri dati sensibili possono emergere dagli Statuti delle associazioni, enti, fondazioni. Queste informazioni, eccetto quelle idonee a rivelare lo stato di salute, possono inoltre essere diffuse ai sensi del D.Lgs. n.267/2000 in ottemperanza al regime di pubblicita' degli atti (pubblicazioni Albo Pretorio). Con riferimento alle attivita' relative alla concessione di benefici, al riconoscimento di benefici il trattamento di dati sensibili si rende necessario sia per la concessione o l'assegnazione stesse, sia per la predisposizione delle graduatorie dei beneficiari, che vengono rese pubbliche ove previsto dalla relativa normativa, fermo restando il divieto di diffondere i dati sulla salute ai sensi degli artt. 22, comma 8, e 68, comma 3, del d.lgs. n. 196/2003. I dati vengono forniti direttamente dagli interessati, che presentano apposita domanda di contributo al Comune, oppure da terzi (anagrafe, autorita' giudiziaria, ASL, provincia, altri servizi comunali, i quali effettuano dei servizi di sostegno in favore dell'utente che versa in stato di indigenza).
Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente

copia informatica per consultazione

all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 37 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo L. 3/3/1951, n.178; art.12 L.241/90; Regolamenti comunali in materia
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 37 - Sistema informativo relativo a concessione di onorificenze, ricompense, contributi, sussidi e benefici - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rilevare convinzioni politiche
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 37 - Trattamento effettuato per finalita' di diritti sociali, politiche sociali e famiglia. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei

copia informatica per consultazione

	processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 37 - Trattamento effettuato per rilevanti finalita' nella seguente materia: conferimento di onorificenze e ricompense, riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali ai sensi dell'art. 2-sexies, comma 2 lett. n) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 37 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): istanti, beneficiari (ai sensi del Regolamento per la concessione di contributi e delle normative nello stesso richiamate)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-nome del dominio del sito web***	
Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server***	
Categorie di interessati	- Persone disabili - Persone fisiche - Persone in cerca di occupazione - Soggetti in difficolta' o pericolo (anche potenziali) - Soggetti con limitata capacita' di intendere e volere - Scolari o studenti di ogni ordine e grado - Rifugiati
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso***	

copia informatica per consultazione

nuove tecnologie	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi

copia informatica per consultazione

	preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche***	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori

copia informatica per consultazione

indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e

copia informatica per consultazione

	utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento

copia informatica per consultazione

accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

  1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
  2 = medio = e' **improbabile** che la minaccia si possa verificare
  3 = alto = = e' **probabile** che la minaccia si possa verificare
  4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

copia informatica per consultazione

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

    - *1 = basso-trascurabile*
    - *2 = medio*
    - *3 = alto*
    - *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e	

copia informatica per consultazione

	relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di

copia informatica per consultazione

	incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4

copia informatica per consultazione

Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Concessione di sovvenzioni, contributi, sussidi, ecc.
Concessione di premi in occasione di manifestazioni sportive
Concessione contributi per manifestazioni
Concessione contributi ad associazioni sportive dilettantistiche
Concessione tariffe agevolate
Concessione contributi ordinari in denaro a sostegno dell'attivita' ordinaria del privato, dell'ente o dell'associazione richiedente

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

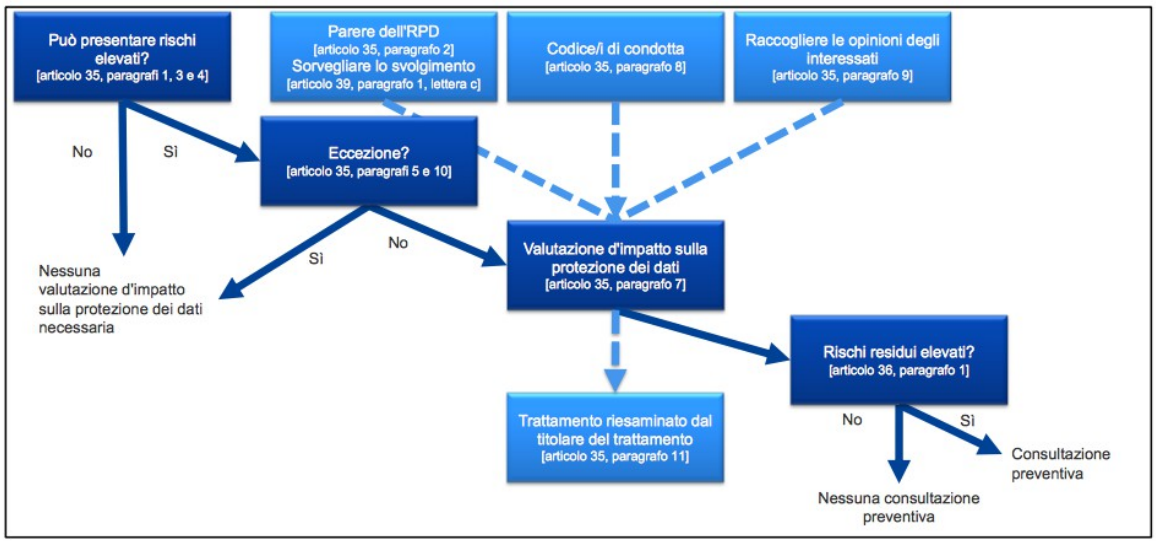
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

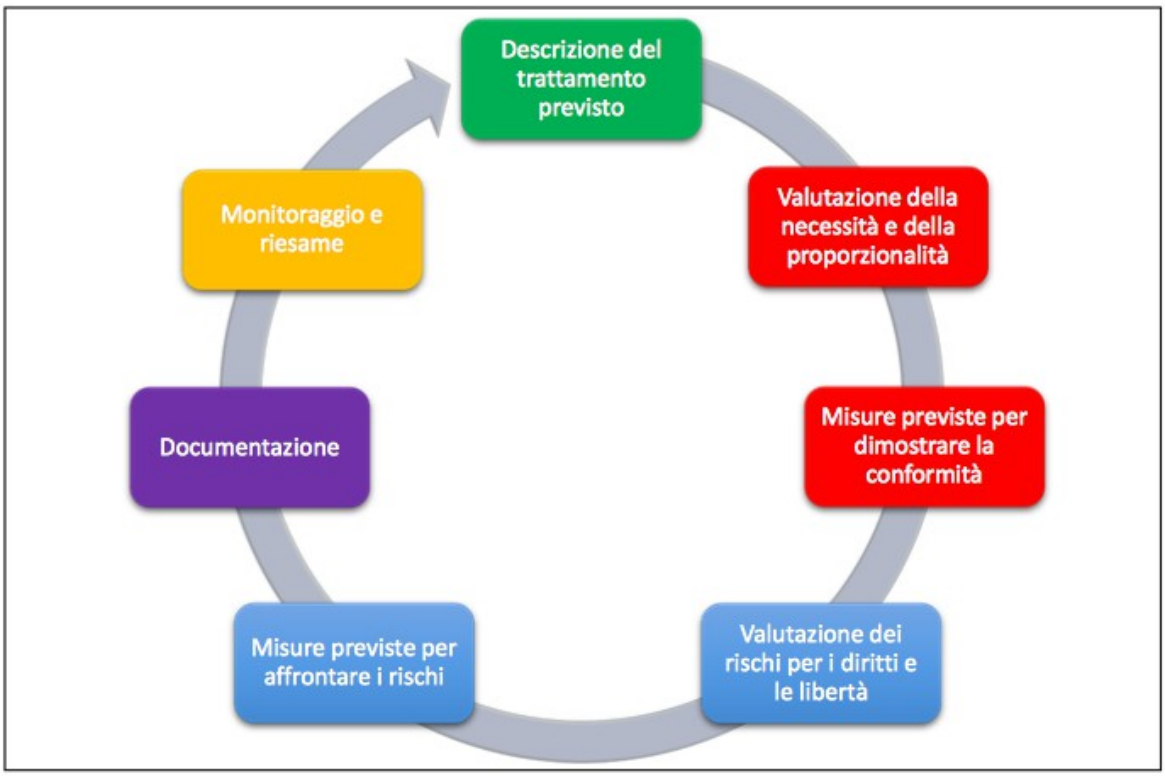
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 39 - I dati vengono raccolti sia presso l'ente, sia presso terzi, sia presso gli interessati allo svolgimento di manifestazioni di pubblico spettacolo, di iniziative culturali od eventi sportivi. Il trattamento puo' includere anche dati vulnerabili e sensibili. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo, basato su sistema di accesso e trasparenza

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 39 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche'

copia informatica per consultazione

	PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo R.D. del 18 giugno 1931, n. 773 TULPS (Testo Unico Leggi Pubblica Sicurezza) Leggi Regionali Regolamenti comunali in materia
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 39 - Sistema informativo relativo ad attivita' ed eventi sportivi - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003)
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 39 - Trattamento effettuato per finalita' culturali o ricreative. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 39 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni ai sensi dell'art. 2-sexies, comma 2 lett. m) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' ricreative o di promozione della cultura e dello sport, incluso l'uso di beni immobili o l'occupazione di suolo pubblico)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli

copia informatica per consultazione

	interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 39 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Comunicazione a Procure del Tribunale in caso di reato nonche' alle Autorita' di volta in volta competenti per le segnalazioni/esposti (ai sensi dell'art. 331 c.p.p.)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Persone fisiche
Categorie di destinatari	- Persone giuridiche, societa' di persone o di capitali, imprese individuali - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare,

copia informatica per consultazione

risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*	gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione

copia informatica per consultazione

Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a

copia informatica per consultazione

	trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di

copia informatica per consultazione

	software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;

copia informatica per consultazione

- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

- **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative	

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un

copia informatica per consultazione

	apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

copia informatica per consultazione

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate

copia informatica per consultazione

Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Rilascio di patrocini
Organizzazione eventi culturali ricreativi
Servizi di gestione impianti sportivi

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

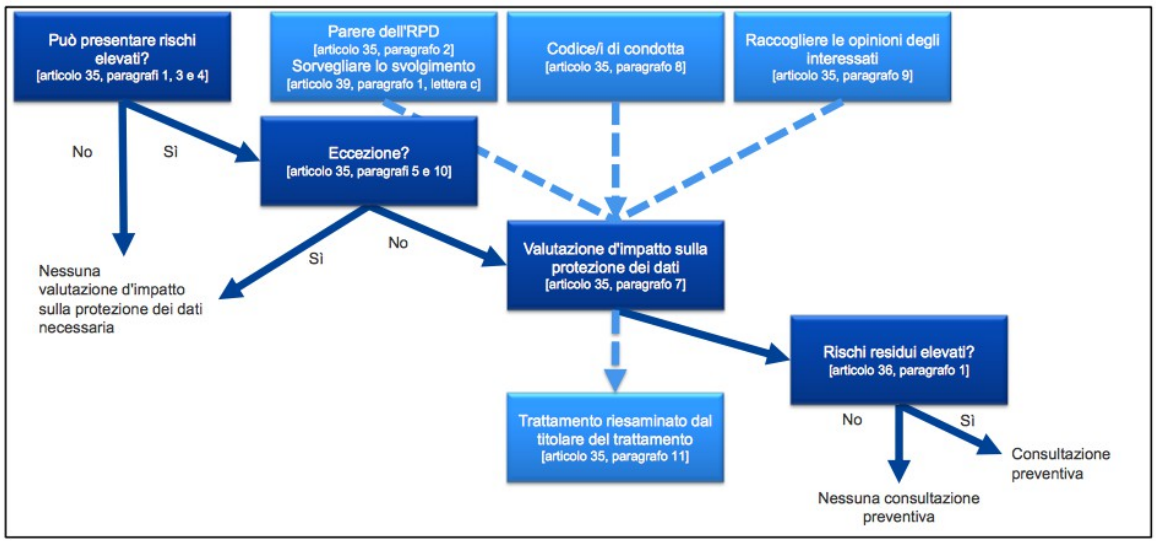
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

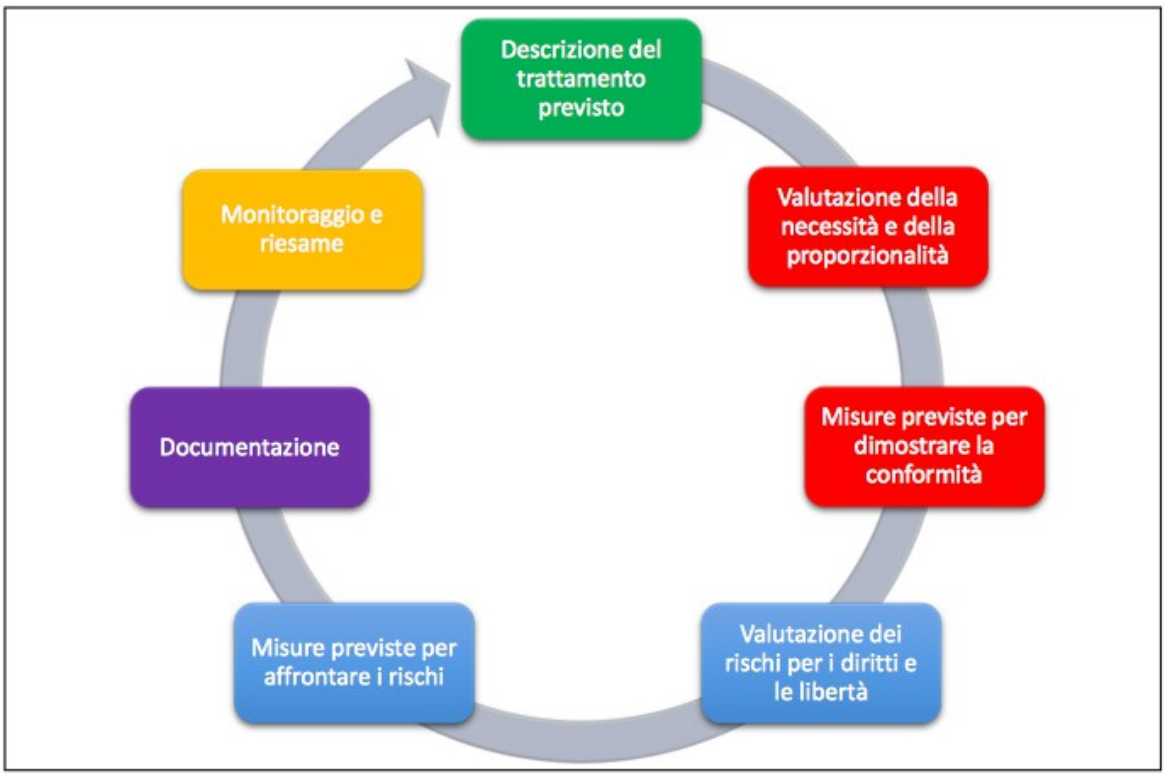
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	R.S.P.P. Responsabile del servizio di prevenzione e protezione
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Dott.ssa Galli M. Cristina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 43 - I dati vengono raccolti presso gli interessati con modalita' elettroniche e su supporti cartacei. Il trattamento, effettuato per rilevanti finalita' di interesse pubblico relative a concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni (art. 68, d.lg. n. 196/2003), puo' includere anche dati vulnerabili e sensibili qualora la richiesta di dilazione di pagamento venga richiesta in ragione di particolare ragioni di disagio sociale ed economico.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 43 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche'

copia informatica per consultazione

	PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - DPR n. 445/2000 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 118/2011 - D.Lgs. 126/2014 Regolamento di contabilita'
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 43 - Base di dati: sistema informativo di gestione della spesa: impegno, liquidazione, ordinazione e pagamento, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati comuni, diversi dai dati particolari - Dati di accesso e di identificazione (user name, password, customer ID, altro) - Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti - Dati sensibili - Dati comuni identificativi - Indirizzo di posta elettronica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 43 - Trattamento effettuato per attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita'	- Scheda n. 43 - Trattamento effettuato per rilevanti finalita' di interesse pubblico

copia informatica per consultazione

di interesse pubblico	nella seguente materia: concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni, ai sensi dell'art. 2-sexies, comma 2 lett. m) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 43 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Tesoriere - Altre amministrazioni per procedimenti connessi (ai sensi del Regolamento di contabilita' e della normativa dallo stesso richiamata)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i*	

copia informatica per consultazione

server	
Categorie di interessati	- Utenti (anche potenziali)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Possibilita' di consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali - Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Liquidazione fatture

21

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

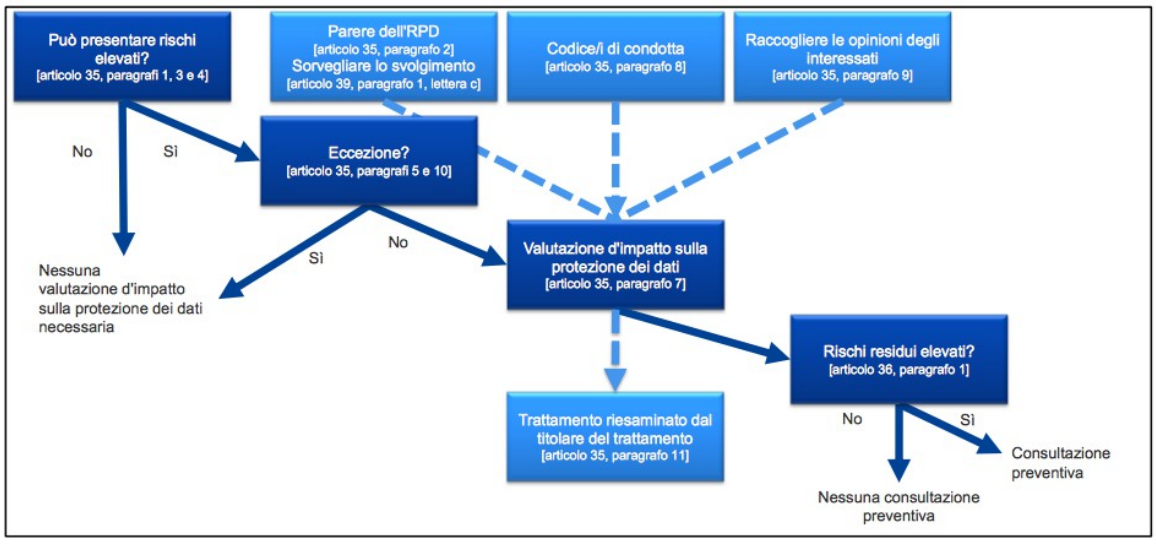
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

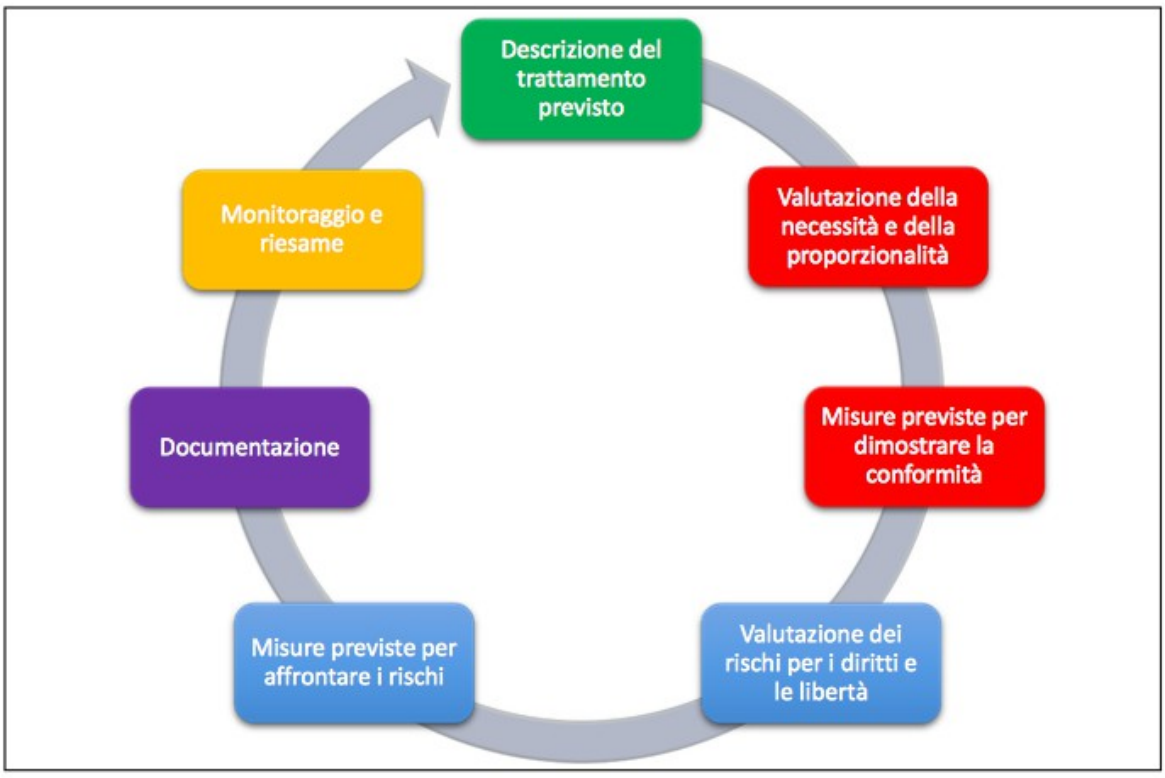
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Cooperativa Sociale C.I.S.S.E.
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 50 - Il trattamento ha per oggetto i dati delle procedure di affidamento e dei contratti di appalto e di concessione delle amministrazioni aggiudicatrici e degli enti aggiudicatori per l'acquisizione di servizi, forniture, lavori e opere, nonche' i concorsi pubblici di progettazione e l'attivita' posta in essere in attuazione del D.Lgs. n. 50/2016. I dati vengono raccolti dai soggetti partecipanti alle procedure di affidamento e includono dati sensibili e giudiziari. Il trattamento implica, oltre alle ordinarie forme di elaborazione standardizzate (con mezzi elettronici e su supporto cartaceo), anche la comunicazione a terzi e, in particolare, alle Autorita' competenti a rilasciare le certificazioni sul possesso dei requisiti, nonche' la possibile diffusione mediante pubblicazione sul profilo del committente e sui siti web prescritti dalla normativa vigente in materia.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 50 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001- Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 50/2016 - Linee Guida Anac - Statuto - Regolamento sul procedimento amministrativo - Regolamento sull'attivita' contrattuale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici - Le attivita' ricomprese in questo trattamento sono le attivita' di competenza trasversalmente, di tutti gli uffici che aggiudicano contratti inclusi nell'ambito di applicazione del D.Lgs. 50 n. 0/2016
Nome archivio/Banca dati	- Scheda n. 50 - Sistema informativo relativo ad appalti, concessioni, autorizzazioni al subappalto contratti di partenariato pubblico privato - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili - Dati relativi al comportamento debitorio - Dati relativi all'affidabilita' o puntualita' nei pagamenti - Dati idonei a rivelare l'origine razziale ed etnica - Dati relativi a comportamenti illeciti o fraudolenti - Dati relativi all'adempimento di obbligazioni - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti - Dati relativi all'affidabilita' nell'esecuzione dei contratti pubblici
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi

copia informatica per consultazione

Finalita' del trattamento	- Scheda n. 50 - Trattamento effettuato per finalita' di adempimento di obblighi contrattuali e precontrattuali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 50 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo, ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (in particolare con riferimento alla verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti- forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 50 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Agenzia Entrate, Prefettura, Tribunale, Procura presso il Tribunale, Provincia e altri enti pubblici - INPS/INAIL/ANAC - , anche attraverso la consultazione delle relative Banche dati, per i controlli sul possesso dei requisiti dichiarati in sede di procedura di affidamento; b) altri soggetti partecipanti alla procedura di affidamento; c) consulenti e soggetti, pubblici o privati, che effettuano servizi di committenza ausiliaria; d) avvocati incaricati dell'eventuale contenzioso (ai sensi del D.Lgs. n. 50/2016 e della regolazione attuativa)
Categorie di trattamenti - particolari forme di elaborazione:	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione sul sito web, in "Amministratrazione trasparente" in attuazione di obblighi di pubblicazione di cui al D. Lgs. n. 33/2013

copia informatica per consultazione

diffusione	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Concorrenti alle procedure di affidamento di contratti pubblici - Soggetti terzi rispetto ai concorrenti, i cui dati rilevano nella procedura di affidamento
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

cartacei o canali di trasmissione	
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II

copia informatica per consultazione

VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la

copia informatica per consultazione

	consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

RISCHI **Origine/fonte dei rischi:** ***accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle

copia informatica per consultazione

	password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC

copia informatica per consultazione

	1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

copia informatica per consultazione

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare	

copia informatica per consultazione

	l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto

copia informatica per consultazione

	- MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione:

copia informatica per consultazione

	FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Convenzioni con Centri di socializzazione
Servizio accreditamenti servizi socio-assistenziali

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO	Servizio Socio Culturale, Sport e Volontariato

TRATTAMENTO	Scheda n. 55 - Servizi Sociali - Trattamento di dati relativi all'attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al "Sistema di protezione dei richiedenti asilo e rifugiati"

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	001
Data ultimo aggiornamento	00/00/0000

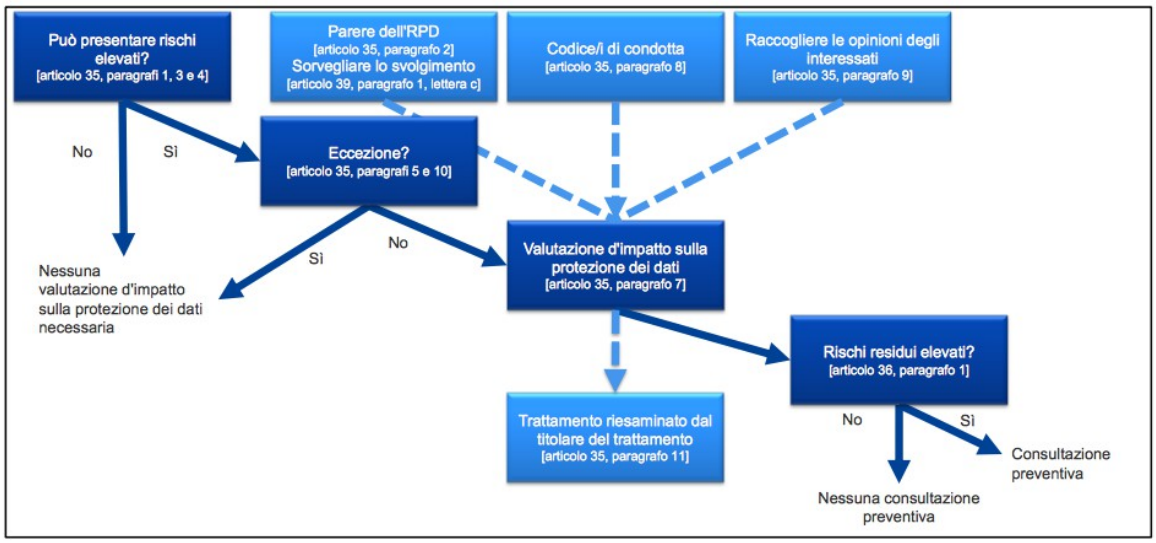
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

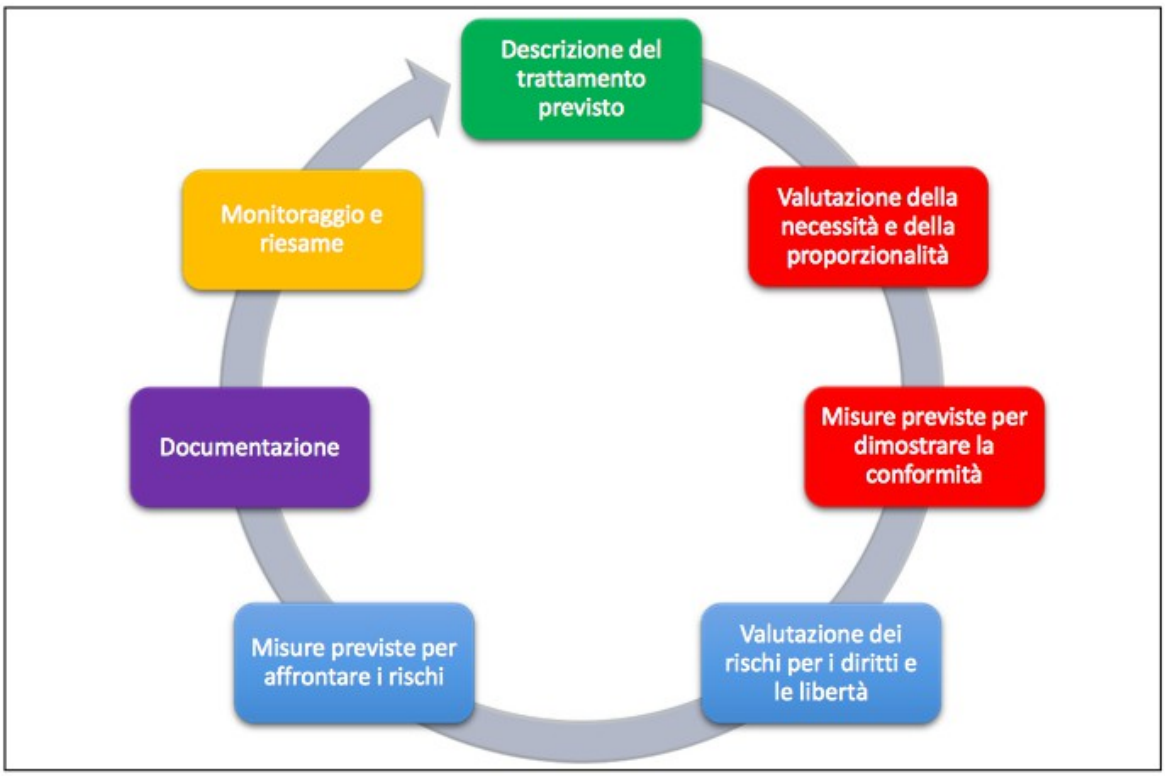
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO
SERVIZIO: denominazione e punti di contatto	Servizio Socio Culturale, Sport e Volontariato
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Sig.ra Avellino Virginia Dott. Tacchella Stefano sig.ra Raino' Chiara

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 55 - Il trattamento ha per oggetto i dati personali relativi alla gestione del Sistema di protezione dei richiedenti asilo e rifugiati (SPRAR). In tale ambito vengono trattati dati giudiziari e dati sensibili, in particolare relativi alla salute dei soggetti interessati.
I dati vengono raccolti, su supporto informatico e cartaceo, presso l'Ente, presso i destinatari e altre pubbliche amministrazioni per finalita' di sicurezza pubblica. Sono oggetto di elaborazione da parte dei competenti uffici comunali e di comunicazione per esigenze di tutela delle persone. Presenti particolari forme di elaborazione: comunicazione a Procure del Tribunale in caso di reato nonche' alle Autorita' di volta in volta competenti per le segnalazioni/ esposti

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 55 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art.

copia informatica per consultazione

	1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.Lgs. 286/1998 - Testo Unico Immigrazione - Statuto - Regolamento sul procedimento amministrativo
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 55 - Sistema informativo relativo a sistema di protezione per richiedenti asilo e rifugiati - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rivelare la vita sessuale (soltanto in caso di rettificazione di sesso) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica - Dati idonei a rilevare patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali - Impronte digitali - Dati idonei a rivelare lo stato di disabilita' - Dati idonei a rivelare il rapporto di parentela o affinita' - Dati idonei a rilevare la posizione di persone - Dati idonei a rilevare lo stato di malattia
Luoghi di custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 55 - Trattamento effettuato per finalita' di sicurezza pubblica. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del

copia informatica per consultazione

	servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 55 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato ai sensi dell'art. 2-sexies, comma 2 lett. e) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al 'Sistema di protezione dei richiedenti asilo e rifugiati')
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 55 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): ad altre amministrazioni (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, vengono trasferiti a un paese terzo o a un'organizzazione internazionale, ed esiste una decisione di adeguatezza della Commissione europea - Trasferimenti consentiti in Paesi terzi
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Immigrati - Rifugiati
Categorie di destinatari	- Soggetti privati - Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine ultimo identificato dalla normativa di settore dello specifico ambito di intervento o, comunque, in base al criterio della cancellazione immediatamente dopo il "periodo minimo indispensabile di trattamento dei dati"

copia informatica per consultazione

Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario,

copia informatica per consultazione

	aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA

copia informatica per consultazione

	VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle

copia informatica per consultazione

	pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di

copia informatica per consultazione

	trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto

copia informatica per consultazione

GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici	

copia informatica per consultazione

	MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

	minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla

copia informatica per consultazione

	protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	FRAMEWORKS FUNZIONE
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai

copia informatica per consultazione

	documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione Responsabile di Posizione Organizzativa individuato in base agli atti di organizzazione, competente per materia a gestire l'attivita' e il trattamento dei dati

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Servizi di integrazione dei cittadini stranieri

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Tributi
SERVIZIO	Servizio Tributi

TRATTAMENTO	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

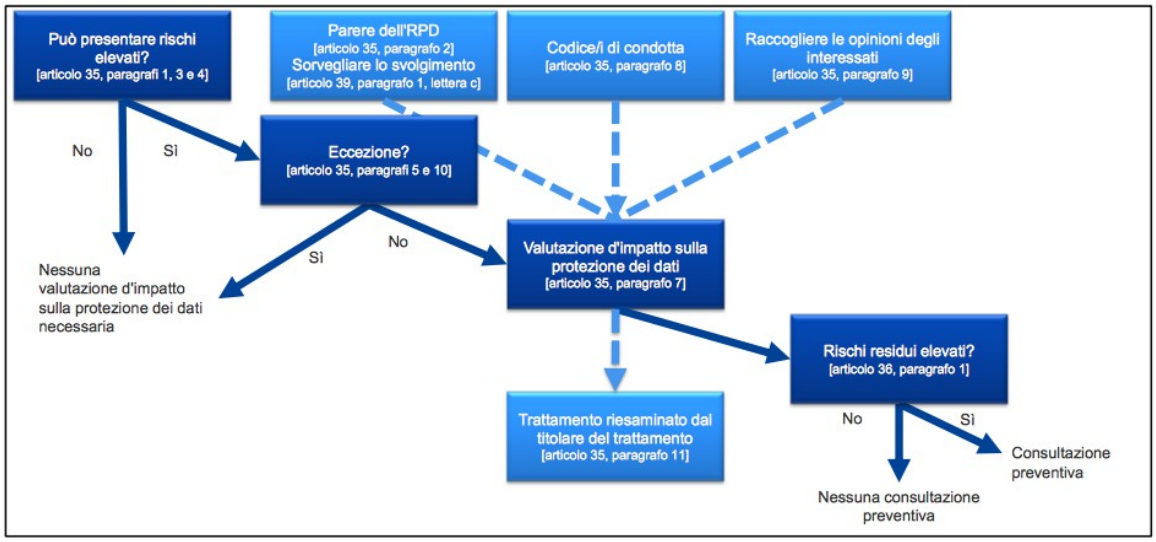
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

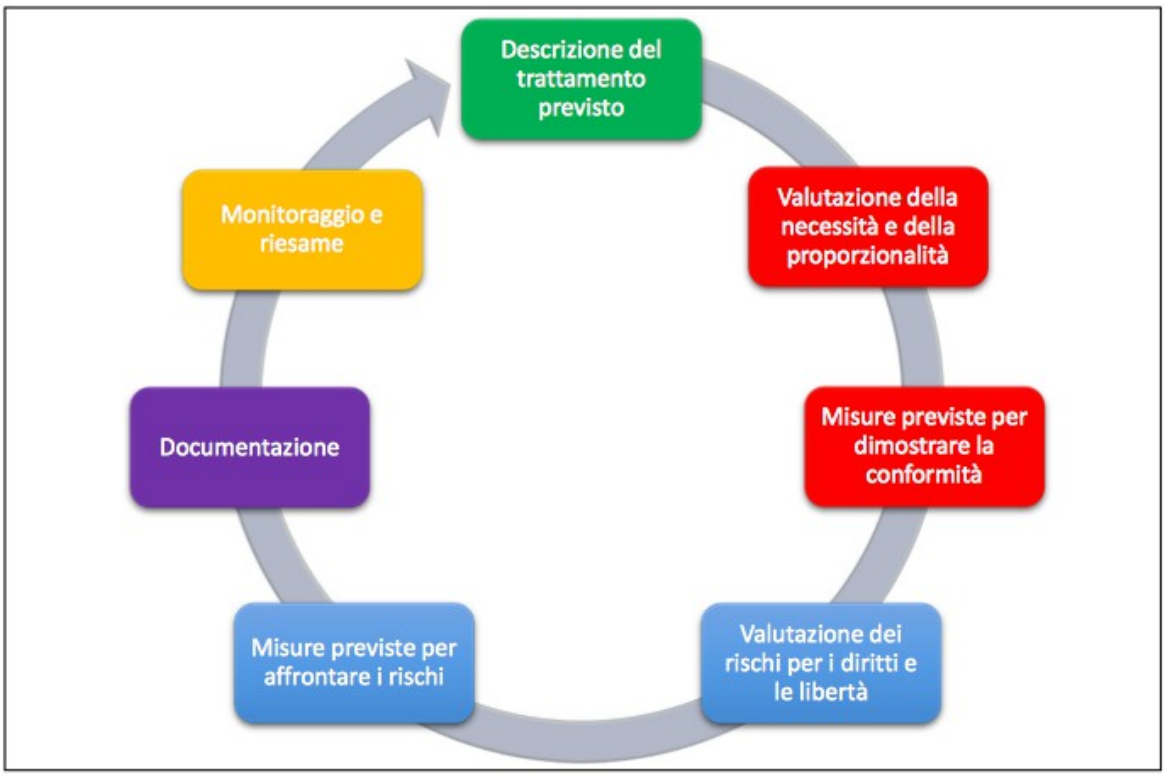
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Tributi
SERVIZIO: denominazione e punti di contatto	Servizio Tributi
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	ETRURIA P.A. SPA
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Servidei Stefano
Incaricati trattamento: denominazione e punti di contatto	sig. Cottone Benedetto sig.ra Ferrini Francesca

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 38 - I dati vengono raccolti sia presso l'ente, sia presso terzi, sia presso gli interessati. Il trattametno puo' includere anche dati vulnerabili e sensibili per finalita' di gestione delle entrate tributarie e servizi fiscali. Vengono effettuate operazioni ordinarie di elaborazione, con mezzi elettronici e su supporto cartaceo e, in relazione ad alcuni trattamenti vengono effettuate anche operazioni particolari di elaborazione per la comunicazione ai seguenti soggetti delle suddette finalita' (con specificazione ed indicazione dell'eventuale base normativa): Agenzia Entrate; Altre pubbliche amministrazioni

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 38 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n.

copia informatica per consultazione

	123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - D.P.R. 380/2001 - Testo Unico delle disposizioni legislative e regolamentari in materia edilizia - Regolamento Edilizio - D.Lgs. 222/2016 - Individuazione di procedimenti oggetto di autorizzazione, SCIA, silenzio-assenso e comunicazione e di definizione dei regimi amministrativi applicabili a determinate attivita' e procedimenti - R.D. 2440/1923 - Leggi finanziarie annuali - Statuto - Regolamento sul procedimento amministrativo - D. Lgs. 504 del 30.12.1992, D. Lgs. 507 del 15.11.1993, L.R. n.96 del 20.12.1996, D.P.R. 118 del 7.04.2000
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 38 - Base di dati: sistema informativo, trattamento fiscale, contributivo e assicurativo, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 38 - Trattamento effettuato per finalita' di servizi istituzionali, generali e di gestione: gestione delle entrate tributarie e servizi fiscali. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 38 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti

copia informatica per consultazione

	riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalita' direttamente connesse all'espletamento di un mandato elettivo ai sensi dell'art. 2-sexies, comma 2 lett. h) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (controllo, di indirizzo politico e di sindacato ispettivo e documentazione dell'attivita' istituzionale di organi pubblici)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 38 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Agenzia Entrate; Altre pubbliche amministrazioni (ai sensi del Regolamenti sui tributi e delle normative nello stesso richiamate)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i*	

copia informatica per consultazione

server	
Categorie di interessati	- Amministrazioni pubbliche di cui all'art. 2, co. 1, D.Lgs. 165/2001
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento:	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa

copia informatica per consultazione

modalita' di cessazione dei dati	comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati

copia informatica per consultazione

	- Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

copia informatica per consultazione

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

copia informatica per consultazione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA'	Alto

copia informatica per consultazione

E GRAVITA' (rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a)

copia informatica per consultazione

	Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Accertamenti e verifiche dei tributi locali
Servizio rilascio certificati relativi a posizioni tributarie
Provvedimenti in autotutela per tributi comunali
Servizio informativo risposte a istanze, comunicazioni, richieste di informazioni opposizioni
Rimborsi a contribuenti - riversamenti a Comuni competenti - sgravi di quote indebite e inesigibili di tributi comunali
Istanze interpello
Accertamenti con adesione dei tributi locali

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Tributi
SERVIZIO	Servizio Tributi

TRATTAMENTO	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

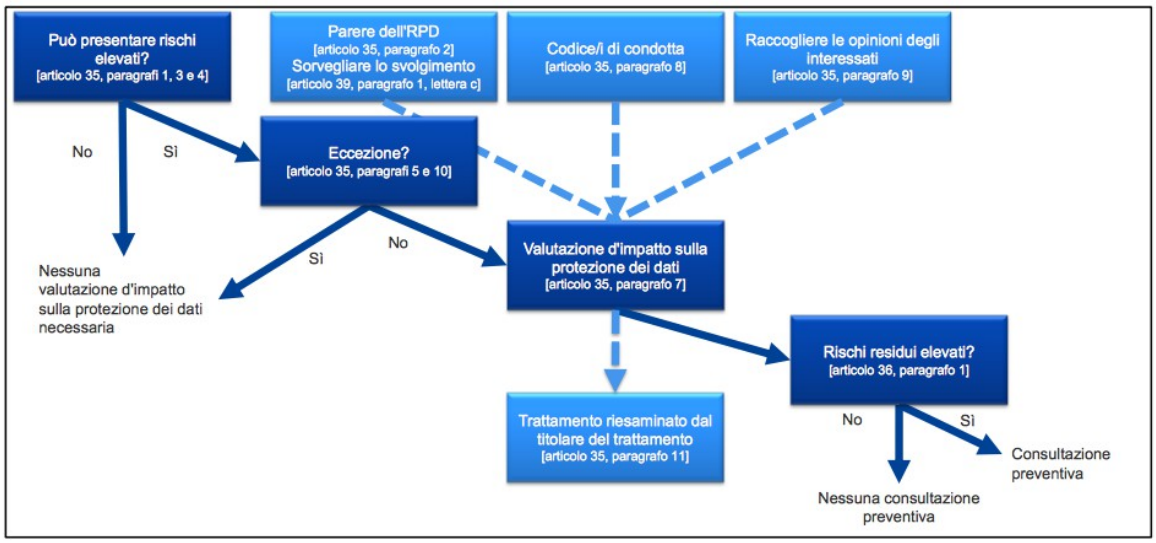
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

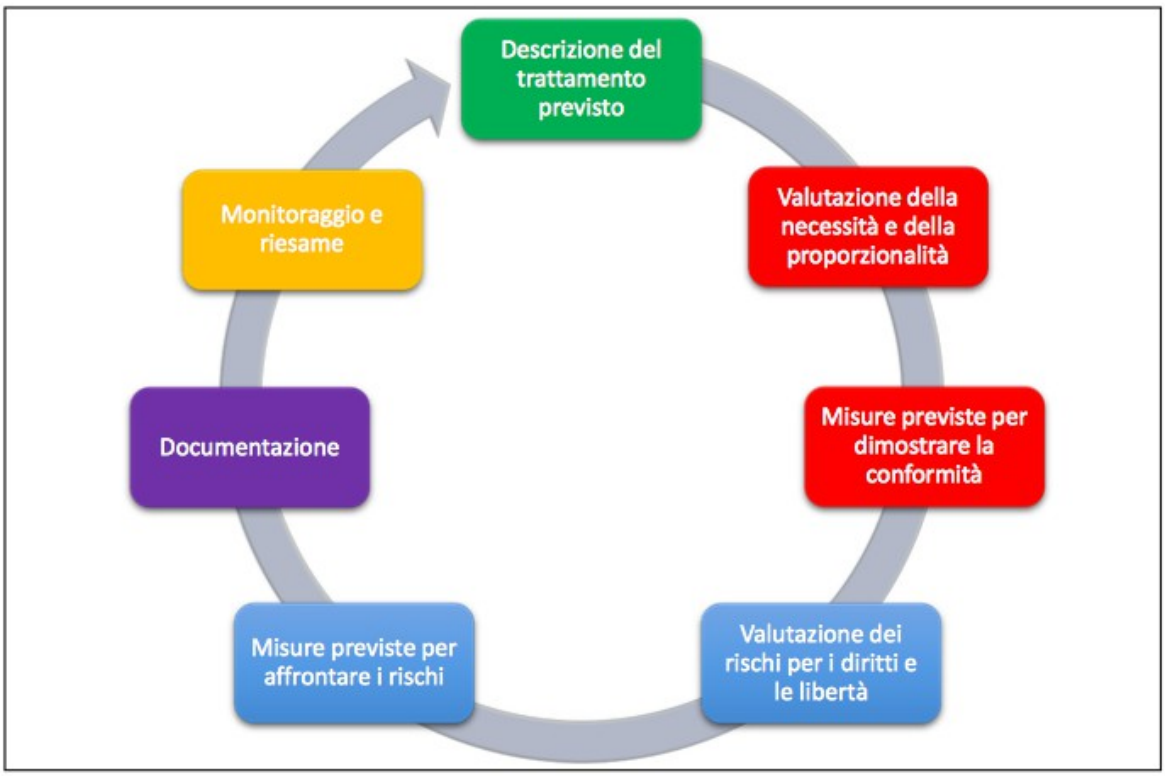
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Tributi
SERVIZIO: denominazione e punti di contatto	Servizio Tributi
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Soggetto affidatario del servizio di riscossione tributaria PUBLISERVIZI SRL I.C.A. - Imposte Comunali Affini S.p.A. ETRURIA P.A. SPA
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Servidei Stefano
Incaricati trattamento: denominazione e punti di contatto	sig. Cottone Benedetto sig.ra Ferrini Francesca

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 42 - I dati vengono acquisiti dagli interessati al momento del sopralluogo e dell'ispezione o verifica; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti o eventuali violazioni rispetto alle dichiarazioni acquisite. I dati sono registrati in archivi/ banche di dati gestite con modalita' elettroniche e su supporti cartacei tramite sistema informativo, controlli esterni, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 42 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 -

copia informatica per consultazione

	D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - D.Lg. n. 50/2016 - Reg. UE 679/2016 - DL. 24 novembre 1981 n. 689 - Statuto - Regolamento sul procedimento amministrativo - Regolamento sui controlli interni
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 42 - Sistema informativo relativo ad autorizzazioni, monitoraggio e controllo - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 42 - Trattamento effettuato per attivita' di controllo, ispettive, comprese le attivita' di sopralluogo. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 42 -Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: attivita' di controllo e ispettive ai sensi dell'art. 2-sexies, comma 2 lett. l) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (attivita' di controllo, ispettive, comprese le attivita' di sopralluogo con la polizia locale)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli

copia informatica per consultazione

	interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 42 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) Autorita' giudiziaria, autorita' di pubblica sicurezza (per accertamenti di carattere giudiziario); b) al RUP e alla stazione appaltante (D.Lgs. n. 50/2016); c) alle autorita' amministrative di vigilanza (D.Lgs. n. 50/2016)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Persone fisiche - Cittadini italiani - Persone giuridiche ed altri enti (comprende societa' di persone) - Cittadini di Paesi appartenenti all'U.E. - Cittadini di Paesi non appartenenti all'U.E.
Categorie di	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di

copia informatica per consultazione

destinatari	cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di cessazione dei dati***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per

copia informatica per consultazione

condotta approvati	quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati

copia informatica per consultazione

Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

copia informatica per consultazione

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E

copia informatica per consultazione

	CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

copia informatica per consultazione

	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Alto
STIMA (XxY) DELLA PROBABILITA'	Alto

copia informatica per consultazione

E GRAVITA' (rilevata dalla prospettiva degli interessati)	

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

 - **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a)

copia informatica per consultazione

	Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Controllo tassa sui rifiuti TARES/TARI

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Tributi
SERVIZIO	Servizio Tributi

TRATTAMENTO	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020

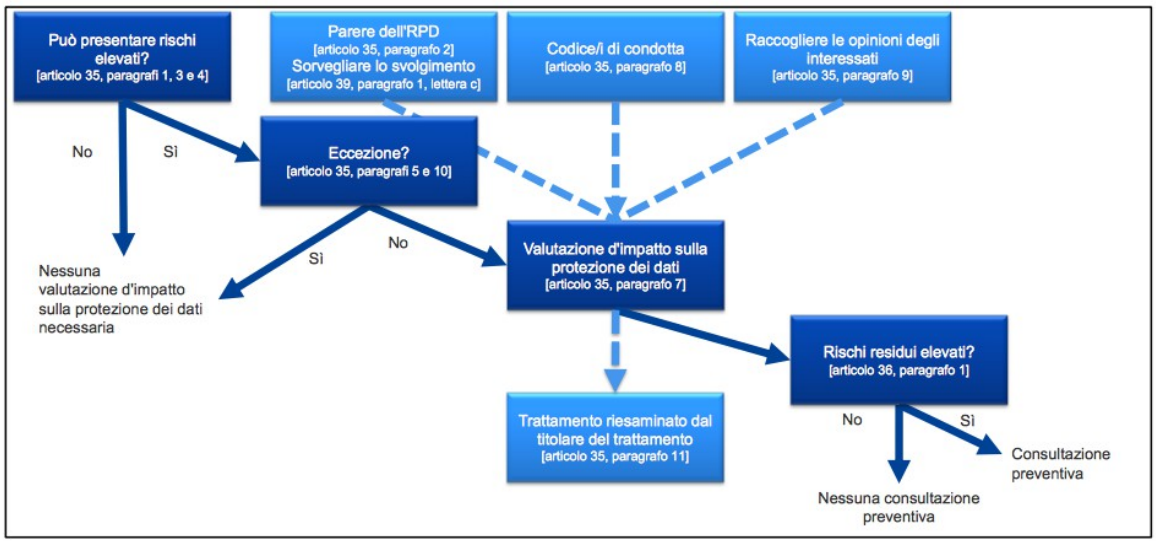
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

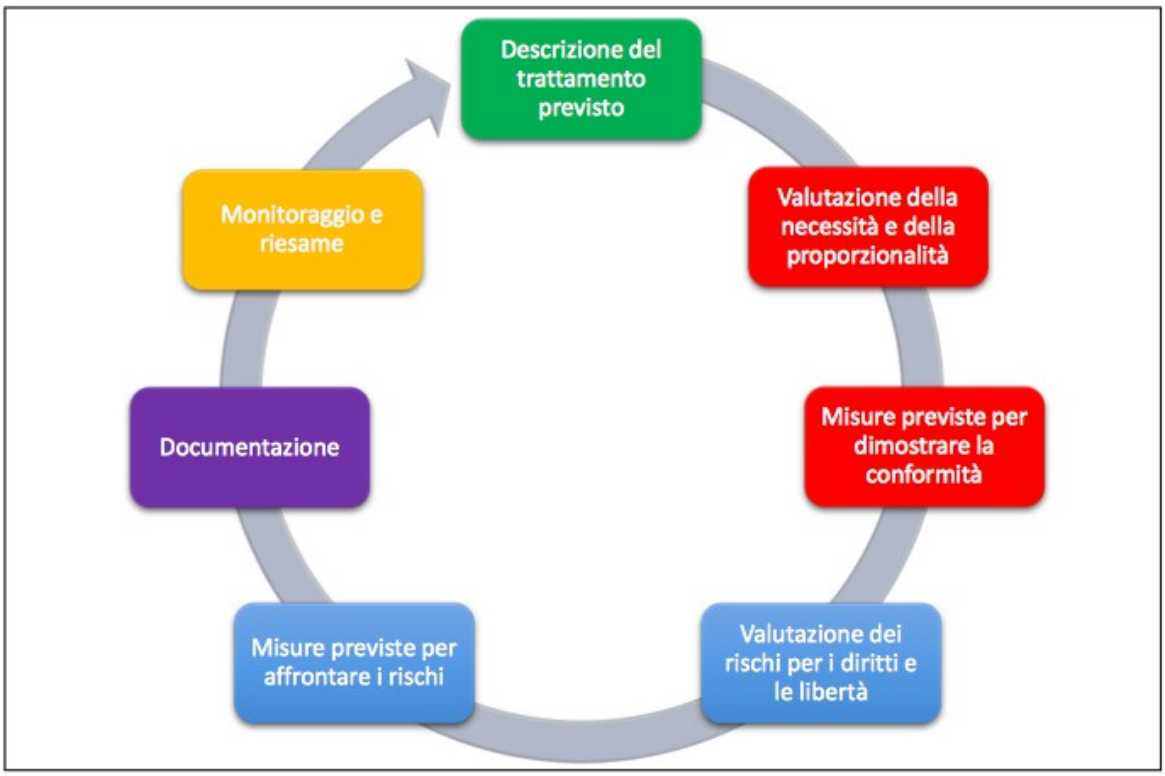
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Servizio Tributi
SERVIZIO: denominazione e punti di contatto	Servizio Tributi
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	PUBLISERVIZI SRL
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Servidei Stefano
Incaricati trattamento: denominazione e punti di contatto	sig. Cottone Benedetto sig.ra Ferrini Francesca

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 43 - I dati vengono raccolti presso gli interessati con modalita' elettroniche e su supporti cartacei. Il trattamento, effettuato per rilevanti finalita' di interesse pubblico relative a concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni (art. 68, d.lg. n. 196/2003), puo' includere anche dati vulnerabili e sensibili qualora la richiesta di dilazione di pagamento venga richiesta in ragione di particolare ragioni di disagio sociale ed economico.

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 43 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche'

copia informatica per consultazione

	PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - DPR n. 445/2000 - Statuto - Regolamento sul procedimento amministrativo D.Lgs. 118/2011 - D.Lgs. 126/2014 Regolamento di contabilita'
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 43 - Base di dati: sistema informativo di gestione della spesa: impegno, liquidazione, ordinazione e pagamento, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati comuni, diversi dai dati particolari - Dati di accesso e di identificazione (user name, password, customer ID, altro) - Dati di carattere giudiziario (art.2-octies D.Lgs. n. 196/2003) - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati relativi al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti - Dati sensibili - Dati comuni identificativi - Indirizzo di posta elettronica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 43 - Trattamento effettuato per attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita'	- Scheda n. 43 - Trattamento effettuato per rilevanti finalita' di interesse pubblico

copia informatica per consultazione

di interesse pubblico	nella seguente materia: concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni, ai sensi dell'art. 2-sexies, comma 2 lett. m) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 43 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): Tesoriere - Altre amministrazioni per procedimenti connessi (ai sensi del Regolamento di contabilita' e della normativa dallo stesso richiamata)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i*	

copia informatica per consultazione

server	
Categorie di interessati	- Utenti (anche potenziali)
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Possibilita' di consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali - Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a)

copia informatica per consultazione

	Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	**FRAMEWORKS FUNZIONE**
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Rateazione pagamento tributi accertati

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	SINDACO
SERVIZIO	Sindaco

TRATTAMENTO	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

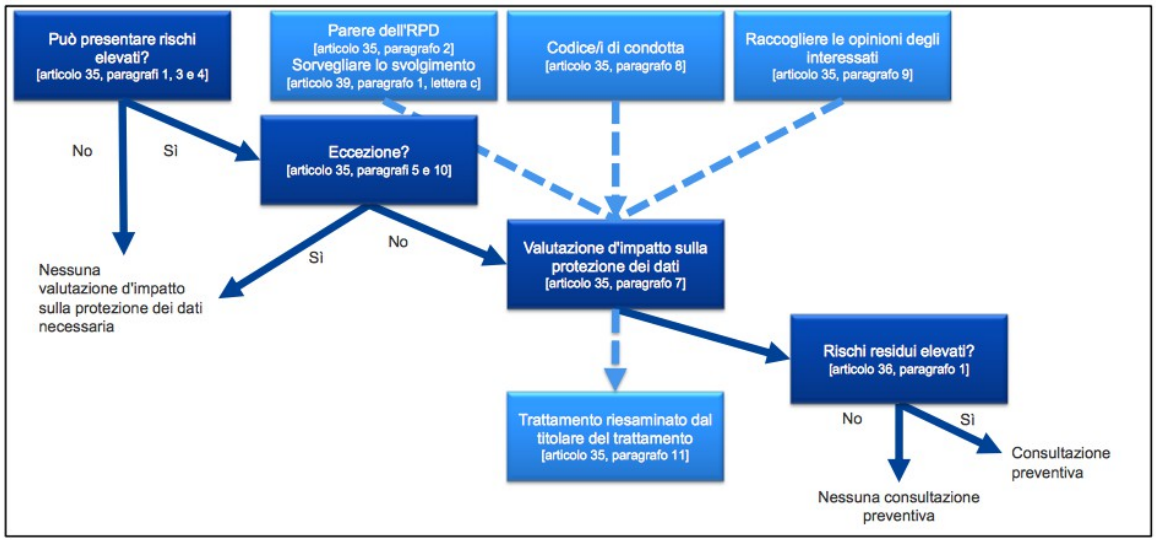
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

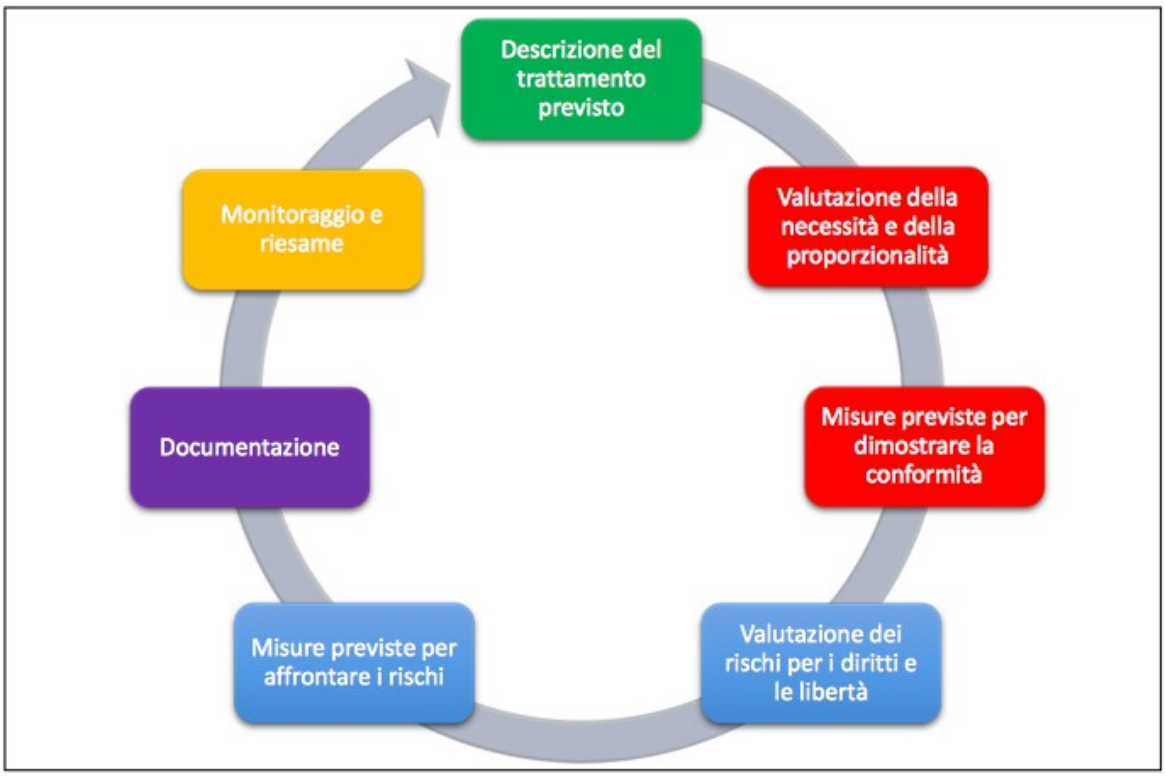
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	SINDACO
SERVIZIO: denominazione e punti di contatto	Sindaco
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 01 - Il trattamento concerne tutti i dati relativi all'instaurazione ed alla gestione del rapporto di lavoro, avviato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'ente ovvero in aziende o istituzioni collegate o vigilate, a partire dai procedimenti concorsuali o da altre procedure di selezione. I dati sono oggetto di trattamento presso le competenti strutture del Comune per quanto riguarda la gestione dell'orario di servizio, le certificazioni di malattie ed altri giustificativi delle assenze; vengono inoltre effettuati trattamenti a fini statistici e di controllo di gestione. I dati sulle convinzioni religiose possono rendersi necessari per la concessione di permessi per quelle festivita' la cui fruizione e' connessa all'appartenenza a determinate confessioni religiose; quelli sulle opinioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza o in relazione a particolari preferenze alimentari, laddove e' previsto un servizio di mensa; le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso. Possono essere raccolti anche dati sulla salute relativi ai familiari del dipendente ai fini della concessione di benefici nei soli casi previsti dalla legge. I dati pervengono su iniziativa dei dipendenti e/o previa richiesta da parte del Comune. I dati vengono trattati ai fini dell'applicazione dei vari istituti contrattuali disciplinati dalla legge (gestione giuridica, economica, previdenziale, pensionistica, attivita' di aggiornamento e formazione). Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 01 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (artt. 2094 - 2134) - D.P.R. 30.06.1965, n. 1124 - L. 20.05.1970, n. 300 - L. 7.02.1990, n. 19 - D.Lgs. 19.09.1994, n. 626 - L. 12.03.1999, n. 68 - Legge 8.03.2000, n. 53 - D.Lgs. 18.08.2000, n. 267 - D.Lgs. 30.03.2001, n. 165 - D.Lgs. 26.03.2001, n. 151 - L. 6.03.2001, n. 64 - D.P.R. 28.12.2000, n. 445 - D.Lgs. 15.08.1991, n. 277 - L. 14.04.1982, n. 164 - CCNL - Contratto collettivo decentrato di ogni singolo ente - Regolamenti comunali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 01 - Sistema informativo relativo alla gestione rapporti contrattuali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rivelare la vita sessuale (soltanto in caso di rettificazione di sesso) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del

copia informatica per consultazione

	dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 01 - Trattamento effettuato per finalita' di gestione del rapporto di lavoro in tutte le sue fasi. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 01 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva ai sensi dell'art. 2-sexies, comma 2 lett. dd) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 01 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) alle organizzazioni sindacali ai fini della gestione dei permessi e delle trattenute sindacali relativamente ai dipendenti che hanno rilasciato delega; b) enti assistenziali, previdenziali e assicurativi e autorita' locali di pubblica sicurezza a fini assistenziali e previdenziali, nonche' per rilevazione di eventuali patologie o infortuni sul lavoro; c) alla Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (d.lgs. n. 165/2001); d) uffici competenti per il collocamento mirato, relativamente ai dati anagrafici degli assunti appartenenti alle "categorie protette"; e) strutture sanitarie competenti per le visite fiscali (art. 5, l. n.

copia informatica per consultazione

	300/1970 e CCNL); f) enti di appartenenza dei lavoratori comandati in entrata (per definire il trattamento retributivo del dipendente); g) Ministero economia e finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600); h) ISPELS (ax art. 70 d.lgs. n. 626/1994)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Personale dipendente - Collaboratori
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware,*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

software, reti, persone, supporti cartacei o canali di trasmissione	
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

copia informatica per consultazione

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati

copia informatica per consultazione

	risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di

copia informatica per consultazione

	software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;

copia informatica per consultazione

- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

- **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita	

copia informatica per consultazione

	l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

C) RISCHIO RESIDUO

RGPD	FRAMEWORKS FUNZIONE
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

copia informatica per consultazione

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Nomina e revoca assessori
Nomina Segretario generale

copia informatica per consultazione

Nomina Organismo di valutazione
Attribuzione e revoca incarichi al personale dirigente

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	00 - AMMINISTRATORI
SERVIZIO	SINDACO
SERVIZIO	Sindaco

TRATTAMENTO	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	

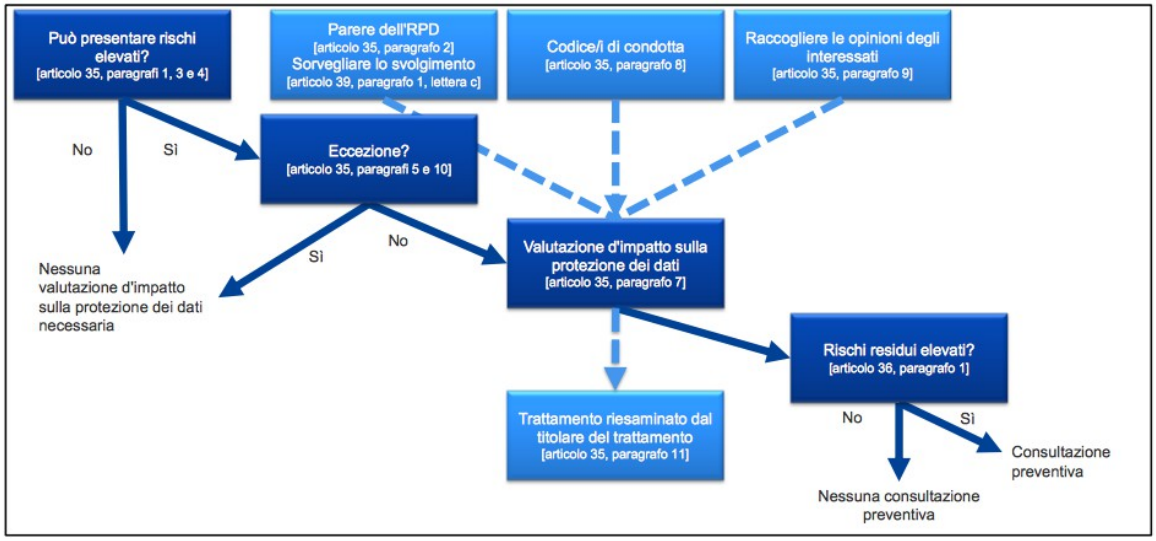
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

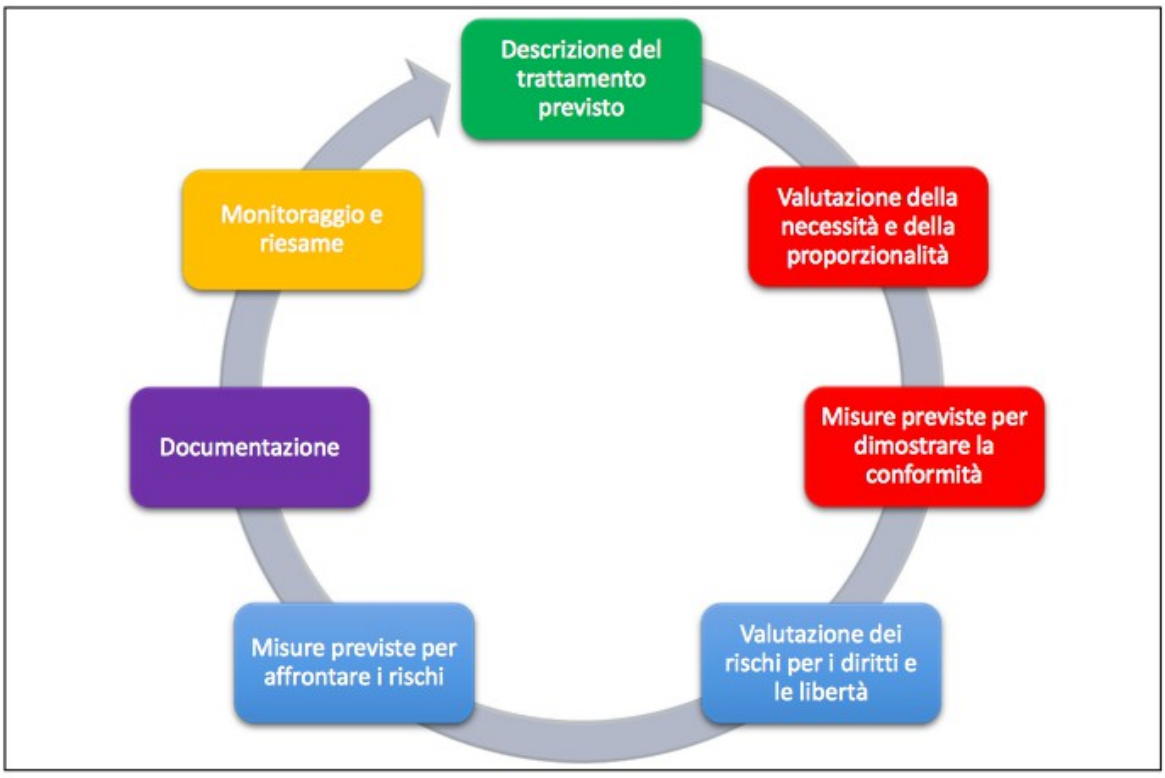
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	00 - AMMINISTRATORI
SERVIZIO	SINDACO
SERVIZIO: denominazione e punti di contatto	Sindaco
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Rossi Antonella
Incaricati trattamento: denominazione e punti di contatto	sig. Mancini Alberto

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 36 - I dati possono essere raccolti sia presso l'interessato, sia presso terzi (ASL, Regione, Provincia, Prefettura, Associazioni di Volontariato di protezione civile, Vigili del Fuoco, Corpo forestale, Autorita' di Pubblica Sicurezza) vengono quindi comunicati ai soggetti coinvolti nelle azioni di intervento, al fine di permettere l'erogazione mirata del servizio. Ai fini della predisposizione della programmazione e dell'adozione dei piani di emergenza in materia di protezione civile, il Comune acquisisce dati inerenti alla dislocazione di strutture e/o abitazioni i cui abitanti, per caratteristiche sanitarie o di disagio psicologico, acquisiscono priorita' in situazioni di emergenza

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 36 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art.

copia informatica per consultazione

	1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D. Lgs. 31 marzo 1998, n. 112, art. 108; Legge 24 febbraio 1992, n. 225, art. 6; Legge 9 novembre 2001, n.401; D.P.R. 8 febbraio 2001 n. 194; Regolamenti comunali in materia
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 36 - Sistema informativo relativo a sicurezza e ordine pubblico - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 36 - Trattamento effettuato per finalita' di protezione civile. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 36 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonche' compiti di igiene e sicurezza sui luoghi di

copia informatica per consultazione

	lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumita' fisica ai sensi dell'art. 2-sexies, comma 2 lett. u) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018 (svolgimento delle competenze che la legge demanda all'Ente locale in materia di protezione civile)
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 36 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) ASL, Aziende ospedaliere e Regioni (per comunicare l'evoluzione della situazione, i controlli e le verifiche periodiche, il monitoraggio dell'attivita'); b) Organi di Polizia / Carabinieri (cui vengono comunicate le attivita' di pubblica sicurezza)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	- Particolari elaborazioni di dati rilevati - Diffusione (con specificazione dell'ambito ed indicazione dell'eventuale base normativa): limitatamente ai dati indispensabili ad assicurare la pubblicazione all'albo pretorio online degli atti (D.Lgs. 267/2000)
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di*	

copia informatica per consultazione

ubicazione del/i server	
Categorie di interessati	- Persone fisiche
Categorie di destinatari	- Altri Uffici/Servizi del titolare (D.Lgs.165/2001) - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 e/o amministrazioni inserite nell'Elenco ISTAT (amministrazioni inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3 della legge 31 dicembre 2009, n. 196) a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg. UE n. 679/2014) - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: ***modalita' di***	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione

copia informatica per consultazione

cessazione dei dati	con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD (art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche,

copia informatica per consultazione

	anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione

copia informatica per consultazione

sicurezza: procedurali	procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

copia informatica per consultazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Ordinanze in qualita' di Ufficiale di governo

20

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Ufficio Gestione economica Personale
SERVIZIO	Ufficio Gestione economica del personale dipendente

TRATTAMENTO	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

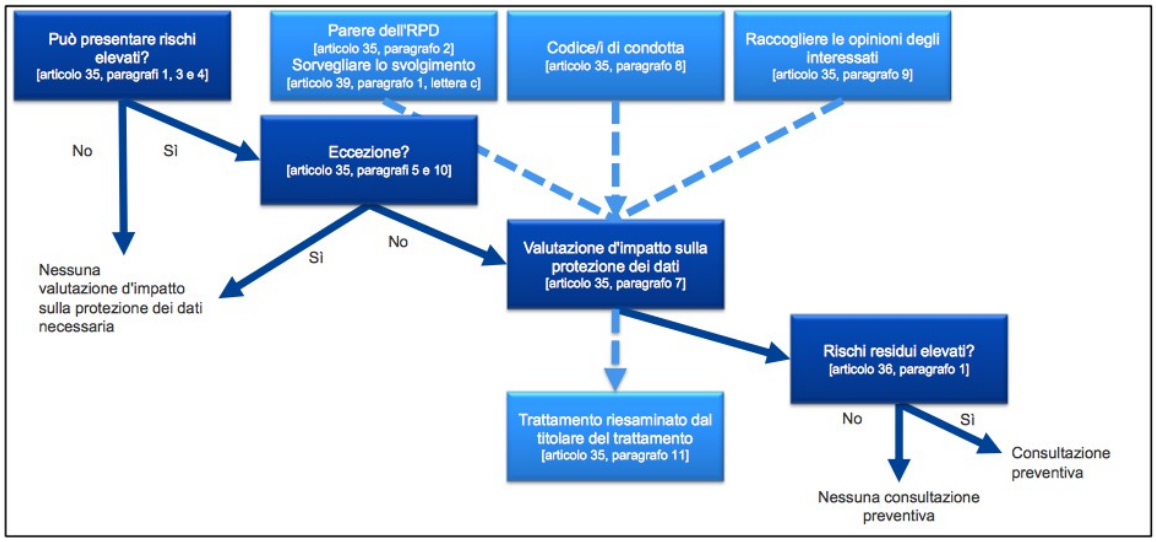
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

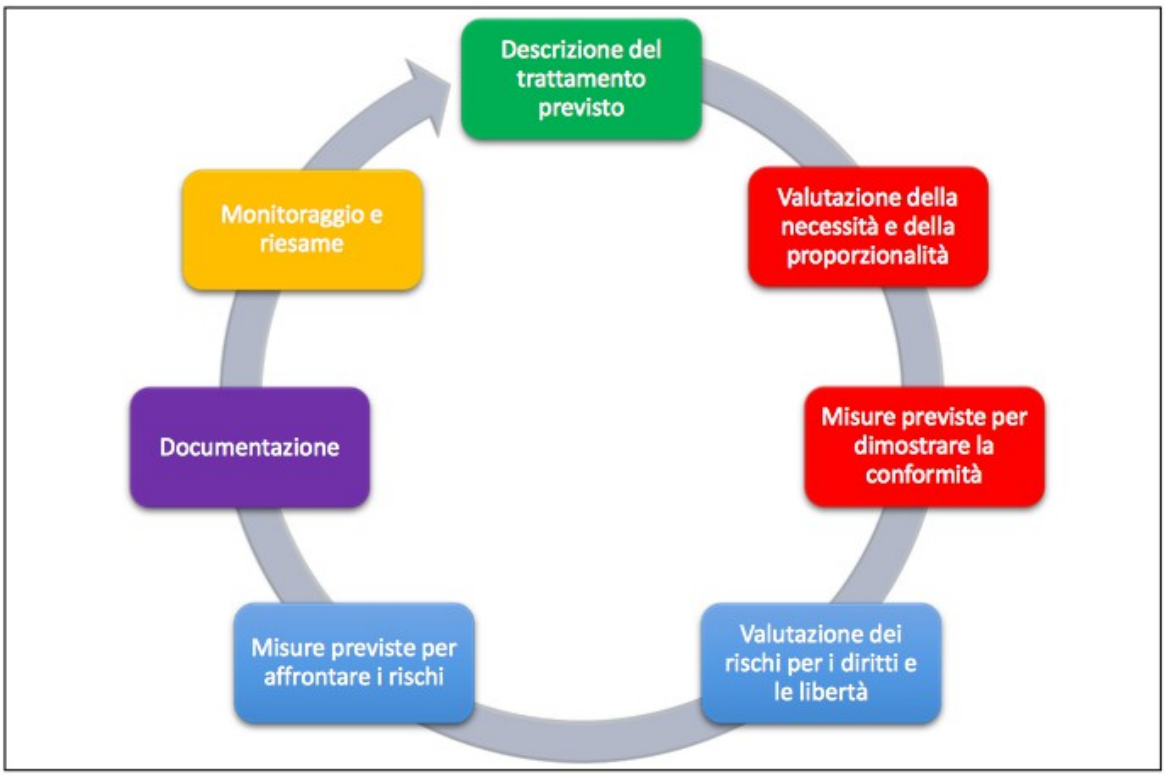
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	03 - AREA FINANZIARIA - TRIBUTARIA
SERVIZIO	Ufficio Gestione economica Personale
SERVIZIO: denominazione e punti di contatto	Ufficio Gestione economica del personale dipendente
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Soggetto affidatario del servizio di elaborazione buste paghe/cedolini dipendenti dell'Ente Consulente del lavoro Girado Gabriella
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott. Servidei Stefano
Incaricati trattamento: denominazione e punti di contatto	Sig. Baldetti Giancarlo sig.ra Ferrini Francesca

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 01 - Il trattamento concerne tutti i dati relativi all'instaurazione ed alla gestione del rapporto di lavoro, avviato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'ente ovvero in aziende o istituzioni collegate o vigilate, a partire dai procedimenti concorsuali o da altre procedure di selezione. I dati sono oggetto di trattamento presso le competenti strutture del Comune per quanto riguarda la gestione dell'orario di servizio, le certificazioni di malattie ed altri giustificativi delle assenze; vengono inoltre effettuati trattamenti a fini statistici e di controllo di gestione. I dati sulle convinzioni religiose possono rendersi necessari per la concessione di permessi per quelle festivita' la cui fruizione e' connessa all'appartenenza a determinate confessioni religiose; quelli sulle opinioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza o in relazione a particolari preferenze alimentari, laddove e' previsto un servizio di mensa; le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso. Possono essere raccolti anche dati sulla salute relativi ai familiari del dipendente ai fini della concessione di benefici nei soli casi previsti dalla legge. I dati pervengono su iniziativa dei dipendenti e/o previa richiesta da parte del Comune. I dati vengono trattati ai fini dell'applicazione dei vari istituti contrattuali disciplinati dalla legge (gestione giuridica, economica, previdenziale, pensionistica, attivita' di aggiornamento e formazione). Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 01 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (artt. 2094 - 2134) - D.P.R. 30.06.1965, n. 1124 - L. 20.05.1970, n. 300 - L. 7.02.1990, n. 19 - D.Lgs. 19.09.1994, n. 626 - L. 12.03.1999, n. 68 - Legge 8.03.2000, n. 53 - D.Lgs. 18.08.2000, n. 267 - D.Lgs. 30.03.2001, n. 165 - D.Lgs. 26.03.2001, n. 151 - L. 6.03.2001, n. 64 - D.P.R. 28.12.2000, n. 445 - D.Lgs. 15.08.1991, n. 277 - L. 14.04.1982, n. 164 - CCNL - Contratto collettivo decentrato di ogni singolo ente - Regolamenti comunali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 01 - Sistema informativo relativo alla gestione rapporti contrattuali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rivelare la vita sessuale (soltanto in caso di rettificazione di sesso) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del

copia informatica per consultazione

	dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 01 - Trattamento effettuato per finalita' di gestione del rapporto di lavoro in tutte le sue fasi. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 01 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva ai sensi dell'art. 2-sexies, comma 2 lett. dd) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 01 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) alle organizzazioni sindacali ai fini della gestione dei permessi e delle trattenute sindacali relativamente ai dipendenti che hanno rilasciato delega; b) enti assistenziali, previdenziali e assicurativi e autorita' locali di pubblica sicurezza a fini assistenziali e previdenziali, nonche' per rilevazione di eventuali patologie o infortuni sul lavoro; c) alla Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (d.lgs. n. 165/2001); d) uffici competenti per il collocamento mirato, relativamente ai dati anagrafici degli assunti appartenenti alle "categorie protette"; e) strutture sanitarie competenti per le visite fiscali (art. 5, l. n.

copia informatica per consultazione

	300/1970 e CCNL); f) enti di appartenenza dei lavoratori comandati in entrata (per definire il trattamento retributivo del dipendente); g) Ministero economia e finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600); h) ISPELS (ax art. 70 d.lgs. n. 626/1994)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Personale dipendente - Collaboratori
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware,*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

software, reti, persone, supporti cartacei o canali di trasmissione	
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

copia informatica per consultazione

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati

copia informatica per consultazione

	risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di

copia informatica per consultazione

	software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;

copia informatica per consultazione

- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

- **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative	

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un

copia informatica per consultazione

	apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione:

copia informatica per consultazione

	FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Stipendi e Paghe

21

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	UFFICIO PERSONALE
SERVIZIO	Ufficio gestione giuridica del personale dipendente

TRATTAMENTO	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD
Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento

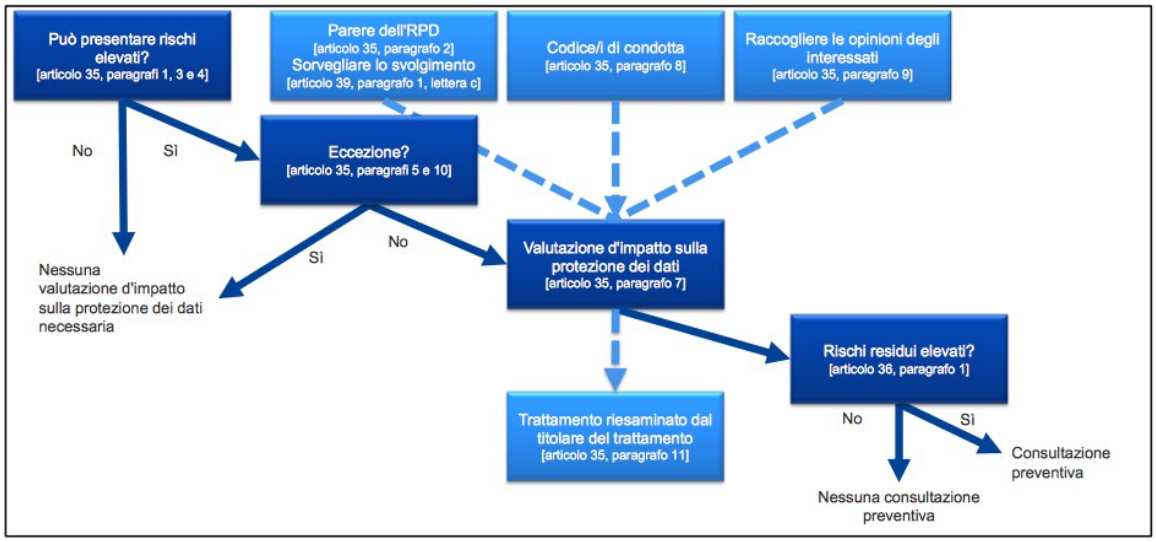
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE
La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

copia informatica per consultazione

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

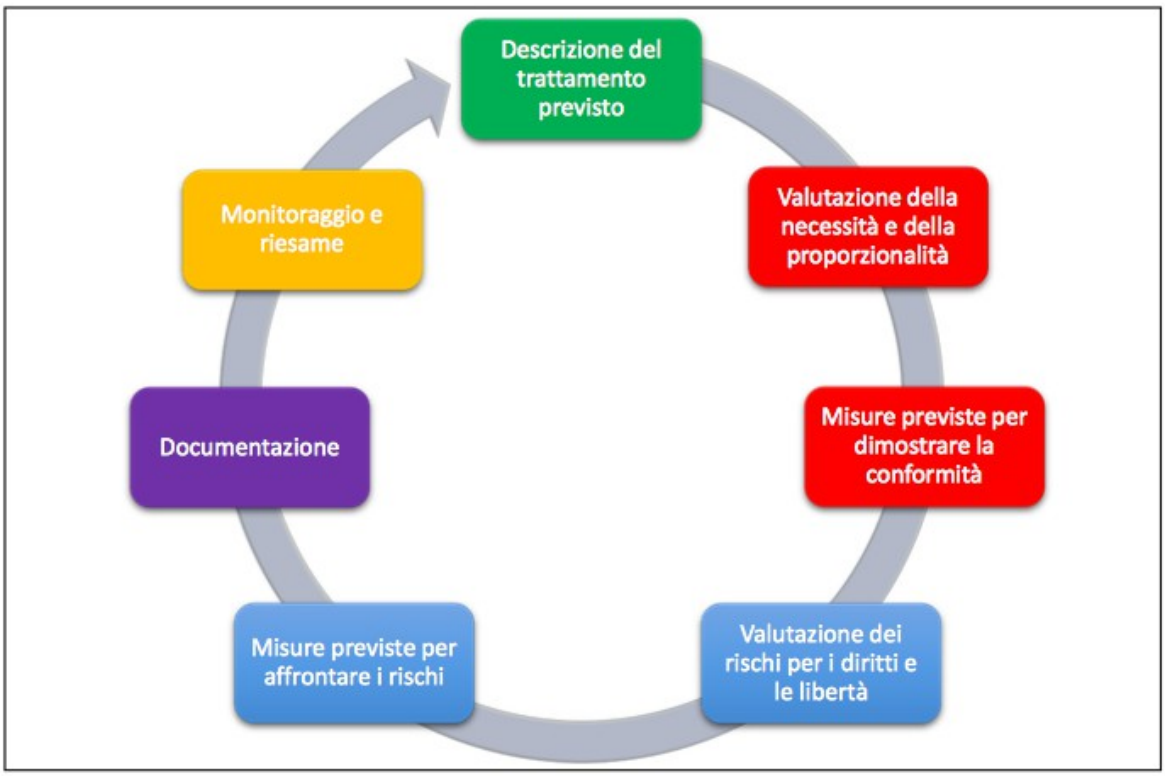
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'

copia informatica per consultazione

compreso, ove applicabile, l'interesse legittimo perseguito dal titolare (art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	UFFICIO PERSONALE
SERVIZIO: denominazione e punti di contatto	Ufficio gestione giuridica del personale dipendente
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	Organismo Indipendente di Valutazione/Componente - Presidente Nucleo di Valutazione Maggioli s.p.a.
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Dott.ssa Galli M. Cristina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 01 - Il trattamento concerne tutti i dati relativi all'instaurazione ed alla gestione del rapporto di lavoro, avviato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'ente ovvero in aziende o istituzioni collegate o vigilate, a partire dai procedimenti concorsuali o da altre procedure di selezione. I dati sono oggetto di trattamento presso le competenti strutture del Comune per quanto riguarda la gestione dell'orario di servizio, le certificazioni di malattie ed altri giustificativi delle assenze; vengono inoltre effettuati trattamenti a fini statistici e di controllo di gestione. I dati sulle convinzioni religiose possono rendersi necessari per la concessione di permessi per quelle festivita' la cui fruizione e' connessa all'appartenenza a determinate confessioni religiose; quelli sulle opinioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza o in relazione a particolari preferenze alimentari, laddove e' previsto un servizio di mensa; le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso. Possono essere raccolti anche dati sulla salute relativi ai familiari del dipendente ai fini della concessione di benefici nei soli casi previsti dalla legge. I dati pervengono su iniziativa dei dipendenti e/o previa richiesta da parte del Comune. I dati vengono trattati ai fini dell'applicazione dei vari istituti contrattuali disciplinati dalla legge (gestione giuridica, economica, previdenziale, pensionistica, attivita' di aggiornamento e formazione). Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

copia informatica per consultazione

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.a)	Descrivere
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Fonte normativa	- Scheda n. 01 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo Codice civile (artt. 2094 - 2134) - D.P.R. 30.06.1965, n. 1124 - L. 20.05.1970, n. 300 - L. 7.02.1990, n. 19 - D.Lgs. 19.09.1994, n. 626 - L. 12.03.1999, n. 68 - Legge 8.03.2000, n. 53 - D.Lgs. 18.08.2000, n. 267 - D.Lgs. 30.03.2001, n. 165 - D.Lgs. 26.03.2001, n. 151 - L. 6.03.2001, n. 64 - D.P.R. 28.12.2000, n. 445 - D.Lgs. 15.08.1991, n. 277 - L. 14.04.1982, n. 164 - CCNL - Contratto collettivo decentrato di ogni singolo ente - Regolamenti comunali
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 01 - Sistema informativo relativo alla gestione rapporti contrattuali - base di dati e applicativo oggetto di comunicazione all'ADIG, in attuazione dell'art. 24-quater, comma 2, D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rivelare la vita sessuale (soltanto in caso di rettificazione di sesso) - Dati idonei a rilevare convinzioni religiose - Dati idonei a rilevare convinzioni filosofiche - Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche) - Dati idonei a rilevare convinzioni politiche - Dati idonei a rilevare convinzioni sindacali - Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso - Dati idonei a rilevare lo stato di salute: dati relativi ai familiari del

copia informatica per consultazione

	dipendente o dell'interessato - Dati idonei a rivelare l'origine razziale ed etnica
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 01 - Trattamento effettuato per finalita' di gestione del rapporto di lavoro in tutte le sue fasi. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare
Rilevanti finalita' di interesse pubblico	- Scheda n. 01 - Trattamento effettuato per rilevanti finalita' di interesse pubblico nella seguente materia: instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva ai sensi dell'art. 2-sexies, comma 2 lett. dd) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 01 - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) alle organizzazioni sindacali ai fini della gestione dei permessi e delle trattenute sindacali relativamente ai dipendenti che hanno rilasciato delega; b) enti assistenziali, previdenziali e assicurativi e autorita' locali di pubblica sicurezza a fini assistenziali e previdenziali, nonche' per rilevazione di eventuali patologie o infortuni sul lavoro; c) alla Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (d.lgs. n. 165/2001); d) uffici competenti per il collocamento mirato, relativamente ai dati anagrafici degli assunti appartenenti alle "categorie protette"; e) strutture sanitarie competenti per le visite fiscali (art. 5, l. n.

copia informatica per consultazione

	300/1970 e CCNL); f) enti di appartenenza dei lavoratori comandati in entrata (per definire il trattamento retributivo del dipendente); g) Ministero economia e finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600); h) ISPELS (ax art. 70 d.lgs. n. 626/1994)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*	
Categorie di interessati	- Personale dipendente - Collaboratori
Categorie di destinatari	- Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware,*	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia

copia informatica per consultazione

software, reti, persone, supporti cartacei o canali di trasmissione	
Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*	
Cessazione trattamento: *Periodo di conservazione dei dati*	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento: *modalita' di cessazione dei dati*	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

copia informatica per consultazione

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati - Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati

copia informatica per consultazione

	risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.c)	**Valutare**

copia informatica per consultazione

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)

copia informatica per consultazione

	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile - APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di

copia informatica per consultazione

	software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)

copia informatica per consultazione

(rilevati dalla prospettiva degli interessati)	
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Alto
GRAVITA' = Y (rilevata dalla prospettiva degli interessati)	Molto alto
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;

copia informatica per consultazione

- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

- *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
- *2 = medio* = e' **improbabile** che la minaccia si possa verificare
- *3 = alto* = = e' **probabile** che la minaccia si possa verificare
- *4 = molto alto* = e' **altamente probabile** che la minaccia si possa verificare

- **IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati

- **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

- *1 = basso-trascurabile*
- *2 = medio*
- *3 = alto*
- *4 = molto alto*

La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

copia informatica per consultazione

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative	

copia informatica per consultazione

	implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un

copia informatica per consultazione

	apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

copia informatica per consultazione

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	FRAMEWORKS FUNZIONE
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	FRAMEWORKS FUNZIONE
art.24	**Documentare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate

copia informatica per consultazione

Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI

Assistenza attivita' di valutazione della performance e assegnazione punteggi e premi degli OIV/Nuclei
Pensioni: Pratiche
Rilascio certificato di stipendio
Statistiche
Rimborso oneri per datore di lavoro
Programma triennale ed annuale del fabbisogno di personale
Concorso per l'assunzione di personale
Selezioni da centro per l'impiego
Stabilizzazioni
Mobilita' dall'esterno ex art. 30 del D.Lgs. 165/2001
Mobilita' ex art. 34 bis, D.Lgs. 165/2001
Mobilita' interna intersettoriale da P.E.G.
Cambi di profilo professionale
Trasformazione del rapporto di lavoro a tempo parziale
Denunce infortuni sul lavoro
Medico competente - nomina
Gestione coperture INAIL
Comandi e trasferimenti

copia informatica per consultazione

Nomina componenti del CUG
Nomina componenti del Nucleo di valutazione - OIV
Rilevazione eccedenze personale
Assunzioni interinali
Attribuzione incarichi dirigenziali
Certificazioni e attestazioni posizioni assicurative (pa) per uso ricongiunzioni, riscatti ed altro
Certificazioni stipendio per cessione quinto - prestiti e cessioni
Concorso per la progressione in carriera del personale
Servizi di formazione del personale dipendente
Sorveglianza sanitaria a cura del medico competente
Conferimento di incarichi di collaborazione, studio e ricerca nonche' di consulenza a soggetti estranei all'amministrazione
Incentivi economici al personale (produttivita' e retribuzioni di risultato)
Gestione giuridica del personale: permessi, ferie, ecc.
Relazioni sindacali (informazione, ecc.)
Sorveglianza sanitaria D. Lgs. 81/2008 - planning visite e certificazioni di idoneita' al lavoro

22

copia informatica per consultazione

Comune di CAMPO NELL'ELBA
Piazza Dante Alighieri n. 1
57034 Marina di Campo LI

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE

DPIA- FASE 2
VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[1]
Documento per provare ed essere in grado di dimostrare che
il trattamento e' effettuato conformemente al RGPD

AREA	02 - Area Amministrativa
SERVIZIO	UFFICIO PERSONALE
SERVIZIO	Ufficio gestione giuridica del personale dipendente

TRATTAMENTO	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa

Abbinamento del trattamento ad un insieme di trattamenti simili	La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*. Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**. L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento.

Titolo del Documento	Singola valutazione di impatto sulla protezione dei dati (DPIA) che esamina un insieme di trattamenti simili che presentano rischi elevati analoghi, redatta conformemente alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 - Documento per provare ed essere in grado di dimostrare che il trattamento e' effettuato conformemente al RGPD

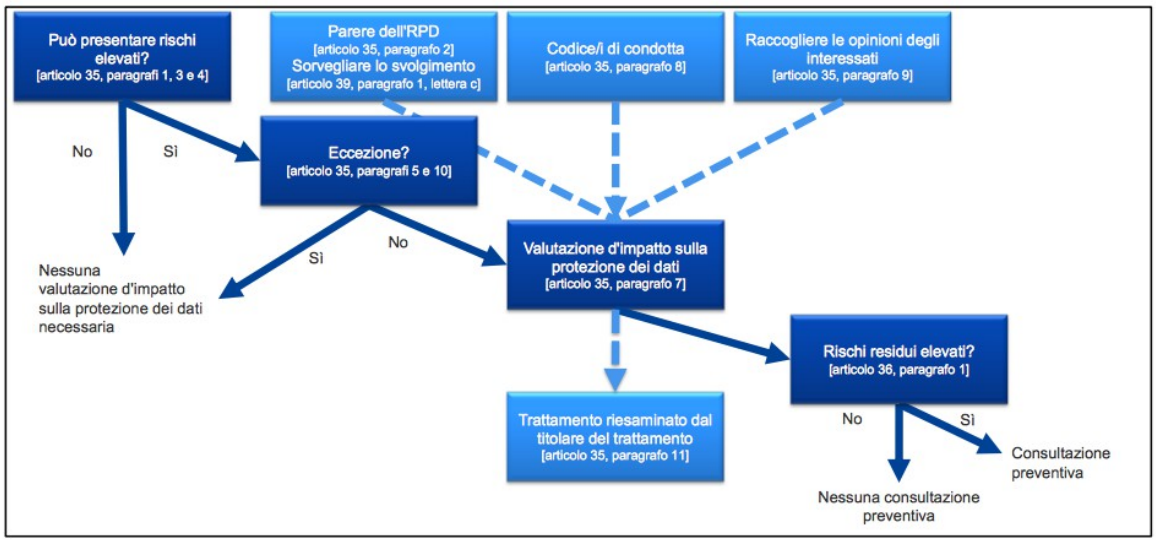
1 Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile"

copia informatica per consultazione

Numero di versione	
Data ultimo aggiornamento	21/04/2020
Stato del documento	Approvato dal titolare con proprio provvedimento
Estensori del documento	- Titolare del trattamento
Riferimento per comunicazioni in merito al documento	- Punti di contatto del titolare del trattamento - TTD
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	- Trasmissione tramite la rete intranet - Conservazione con supporto informatico

RISCHIO ELEVATO E OBBLIGO DI DPIA

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").
La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.
La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

OBIETTIVI DA RAGGIUNGERE

copia informatica per consultazione

La DPIA e' funzionale alla gestione del rischio[2], per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.
L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". Il riferimento a "*diritti e liberta'"* degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.
In questo quadro, la DPIA intende fungere da strumento:

- che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
- che consente di comprovare la conformita' del sistema al RGPD.

DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

- assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA

- raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate

- documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
- se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)

- sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

- assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

2 Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative.

copia informatica per consultazione

CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA

Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology(modello COBITS) nonche' degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del RGPD :

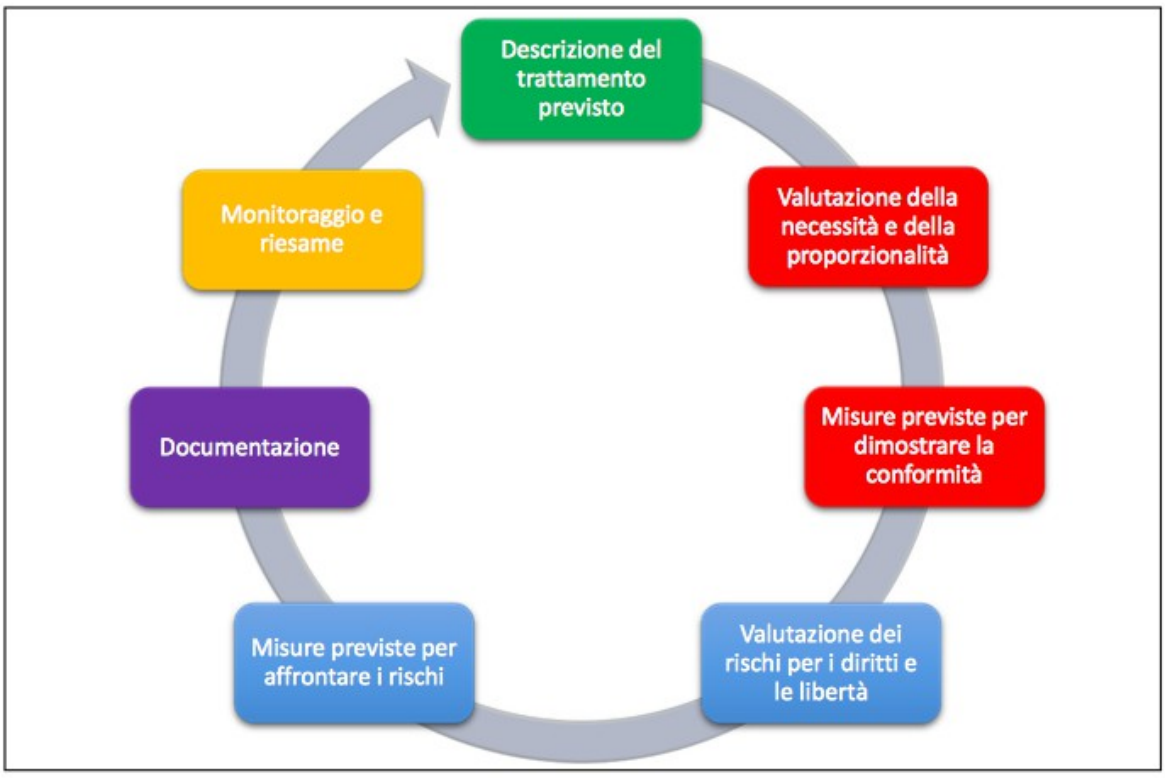
a) una **descrizione sistematica** dei trattamenti previsti e delle finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una **valutazione** della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

c) una **valutazione dei rischi** per i diritti e le liberta' degli interessati di cui al paragrafo 1; e

d) le **misure** previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

copia informatica per consultazione

SEZIONE I
DESCRIZIONE SISTEMATICA
DEL TRATTAMENTO PREVISTO E DELLE FINALITA'
compreso, ove applicabile, l'interesse legittimo perseguito dal titolare
(art. 35, paragrafo 7, lettera a)

AREA	02 - Area Amministrativa
SERVIZIO	UFFICIO PERSONALE
SERVIZIO: denominazione e punti di contatto	Ufficio gestione giuridica del personale dipendente
Titolare trattamento: denominazione e punti di contatto	Comune di CAMPO NELL'ELBA Sindaco Montauti Davide
Contitolare/i trattamento: denominazione e punti di contatto	
Responsabile trattamento: denominazione e punti di contatto	
Sub-Responsabile: denominazione e punti di contatto	
Delegato trattamento: denominazione e punti di contatto	Dott.ssa Mazzanti Agnese
Incaricati trattamento: denominazione e punti di contatto	Dott.ssa Galli M. Cristina

Sintetica descrizione del trattamento e del flusso informativo

Scheda n. 02 - I dati vengono acquisiti dall'interessato e da terzi previa richiesta dell'interessato (in particolare dalla Commissione medico ospedaliera territorialmente competente per l'accertamento delle condizioni di idoneita' al servizio e dal Comitato di verifica per le cause di servizio in caso di richiesta di riconoscimento di invalidita' dipendente da causa di servizio e/o equo indennizzo). In caso di richiesta di pensione privilegiata, i dati vengono trasmessi all'Inpdap per l'erogazione del trattamento pensionistico. Uguale trasmissione si ha nell'ipotesi di richiesta di riconoscimento alla contribuzione figurativa di cui all'art. 80, l. n. 388/2000. Esperita l'istruttoria, la determinazione dirigenziale relativa al riconoscimento dell'invalidita' viene comunicata all'INPS o alle Regioni (per gli accertamenti connessi alla liquidazione ai sensi dell'art. 130 d.lg. n. 112/1998). Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000

RGPD	FRAMEWORKS FUNZIONE

copia informatica per consultazione

art.35 lett.a)	Descrivere

CRITERI LINEE GUIDA	DPIA TRATTAMENTO
Fonte normativa	- Scheda n. 02 - Principi dell'ordinamento dell'Unione europea e normativa europea pertinente - Costituzione - Principi generali dell'attivita' amministrativa di cui all'art. 1, L. 241/1990 - Disposizioni che attengono ai livelli essenziali delle prestazioni (LEA), di cui all'articolo 117, secondo comma, lettera m), Cost. - D.Lgs. n. 267/2000 - D.Lgs. n. 165/2001 - Legge n. 145/2002 - D.Lgs. n. 196/2003 - D.Lgs. n. 82/2005 - D.Lgs. 193/2006 - D.Lgs. n. 150/2009 - L. 69/2009 - D.Lgs. n. 104/2010 - D.Lgs. n. 123/2011 - D.Lgs. n. 149/2011 - L. 190/2012 - PNA 2013, e successivi nonche' PTPC in vigore - D.Lgs. n. 33/2013 - DPR n. 62/2013 e Codice di comportamento dell'Ente - L. 124/2015 e decreti legislativi attuativi - Reg. UE 679/2016 - Statuto - Regolamento sul procedimento amministrativo D.P.R. 30.06.1965, n. 1124 - L. 24.05.1970, n. 336 - Legge 5.02.1992, n. 104 - L. 12.03.1999, n. 68 - D.P.R. 29.10.2001, n. 461 - L. 8.08.1995, n. 335 - L. 8.03. 1968, n. 152 - Legge regionale - regolamento comunale in materia di organizzazione del personale
Natura del trattamento	- Conferimento obbligatorio per le finalita' sopra indicate: l'eventuale rifiuto comporta l'impossibilita' di eseguire il trattamento dei dati e di gestire il processo/procedimento nel cui contesto vanno trattati i dati
Ambito di applicazione del trattamento	- Ambito di applicazione materiale e territoriale individuato in base agli artt. 2 e 3 del Regolamento (UE) 679/2016 - Trattamento in ambito pubblico - Ambito identificato dal profilo di autorizzazione consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
Nome archivio/Banca dati	- Scheda n. 02 - Base di dati: sistema informativo gestione giuridica del personale, comunicata all'Agenzia per l'Italia digitale in attuazione dell'art. 24-quater, comma 2, del D.L. n. 90/2014, convertito in L. n. 114/2014
Tipo di archivio/Banca dati	- I dati sono registrati in archivi/banche di dati gestite con modalita' in prevalenza elettroniche e con supporti cartacei
Categorie-tipi di dati	- Dati idonei a rilevare lo stato di salute: patologie attuali - Dati idonei a rilevare lo stato di salute: patologie pregresse - Dati idonei a rilevare lo stato di salute: terapie in corso
Luoghi di custodia dei dati	- In Italia - Presso l'ubicazione dell'Ufficio competente, come identificato nella MAPPA dei luoghi
Finalita' del trattamento	- Scheda n. 02 - Trattamento effettuato per finalita' di gestione del rapporto di lavoro in tutte le sue fasi. I dati acquisiti vengono trattati esclusivamente per la finalita' di gestione del processo/procedimento amministrativo per il quale vengono comunicati, incluse le fasi di controllo e monitoraggio, e possono essere trattati anche per la gestione dei processi/procedimenti connessi e trasversali, e relativi al controllo di qualita' del servizio e alla misurazione e valutazione della performance. I dati possono essere trattati, altresi', per adempiere ad eventuali obblighi previsti dalla legislazione europea, dalla legislazione italiana, statale e regionale e dalla vigente normativa regolamentare

copia informatica per consultazione

Rilevanti finalita' di interesse pubblico	- Scheda n. 02 - Trattamento effettuato per rilevanti finalita' di interesse pubbliconella seguente materia: concessione, liquidazione modifica e revoca di benefici economici, agevolazioni, elargizioni, emolumenti ai sensi dell'art. 2-sexies, comma 2 lett. m) D.Lgs. n. 196/2003 come modificato dal D.Lgs. n. 101/2018
Interesse legittimo perseguito	- Non si applica al trattamento di dati effettuato dalle autorita' pubbliche, nell'esecuzione dei loro compiti, la condizione di liceita' del legittimo interesse (in forza del quale il trattamento e' lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: .... f) e' necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le liberta' fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato e' un minore)
Categorie di trattamenti-forme ordinarie di elaborazione	Raccolta presso gli interessati Elaborazione in forma cartacea Elaborazione con modalita' informatizzate Raccolta presso terzi
Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*	- Scheda n. 02 - Particolari forme di elaborazione - Comunicazione ai seguenti soggetti per le seguenti finalita' (con specificazione ed indicazione dell'eventuale base normativa): a) INAIL (per verificare la liquidazione in caso di equo indennizzo ai sensi del d.P.R. n. 1124/1965); b) comitato di verifica per le cause di servizio e commissione medica territorialmente competente (per conseguire il parere definitivo di riconoscimento della causa di servizio ai sensi del d.P.R. n. 461/2001); c) INPDAP (in caso di inabilita' assoluta e permanente a qualsiasi attivita' lavorativa ai fini dell'erogazione del relativo trattamento di pensione e del riconoscimento del diritto alla pensione privilegiata ai sensi della l. n. 335/1995 e della l. n. 152/1968)
Categorie di trattamenti - particolari forme di elaborazione: *diffusione*	N.R.
Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*	- I dati personali, oggetto di trattamento, non vengono trasferiti a un paese terzo o a un'organizzazione internazionale
Categorie di trattamenti - particolari forme di elaborazione: *trattamento effettuato tramite un sito web-nome del dominio del sito web*	

copia informatica per consultazione

Categorie di trattamenti - particolari forme di elaborazione: ***trattamento effettuato tramite un sito web- Paese/i di ubicazione del/i server***	
Categorie di interessati	- Personale dipendente - Dirigenti e dipendenti
Categorie di destinatari	- Organismi del servizio sanitario nazionale - Amministrazioni pubbliche di cui all'art. 2, co.1 D.Lgs. 165/2001 - Soggetti privati a cui i dati vanno comunicati per assolvere alla finalita' del trattamento, e che possono assumere il ruolo di responsabile, contitolare o titolare autonomo del trattamento (artt. 26 e 28 Reg.UE n. 679/2014)
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***hardware, software, reti, persone, supporti cartacei o canali di trasmissione***	Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia
Strumenti e risorse coinvolti nel trattamento dei dati personali: ***uso nuove tecnologie***	
Cessazione trattamento: ***Periodo di conservazione dei dati***	- I dati sono conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Cessazione trattamento: ***termine ultimo per la cancellazione delle diverse categorie di dati***	- Termine identificato dalla disciplina specifica di settore e, in particolare, dal vigente Regolamento sul procedimenti amministrativi o, comunque, termine identificato in base al CRITERIO del rispetto del principio di limitazione della conservazione (art.5, par.1, lett. e), GDPR), in forza del quale i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalita' per le quali sono trattati; i dati personali possono essere conservati per periodi piu' lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle liberta' dell'interessato (limitazione della conservazione)
Cessazione trattamento:	- Conservazione per scopi istituzionali, in conformita' alle norme di legge sulla conservazione della documentazione amministrativa, ai regolamenti, alla normativa

copia informatica per consultazione

modalita' di cessazione dei dati	comunitaria e ai codici di deontologia e buona condotta, e successiva archiviazione con eventuale trasmissione dei dati, in conformita' alla legge e ai regolamenti, ai responsabili che effettuano l'archiviazione
Parere RPO/RTD	- E' stato acquisito il parere del RPD, che viene allegato al presente documento di valutazione di impatto
Opinioni interessati o loro rappresentanti	- E' stata effettuata la consultazione pubblica allo scopo di acquisire l'opinione degli interessati che viene allegata al presente documento di valutazione
Rispetto codici di condotta approvati	- Si rinvia ai Codice di deontologia e di buona condotta approvati dal Garante, per quanto applicabili, nonche' al Codice di comportamento approvato con D.P.R. n. 62/2013 e al Codice di comportamento interno approvato dal titolare ad integrazione del D.P.R. n. 62/2013
Adesione ad un meccanismo di certificazione	- Non risulta l'adesione a un meccanismo di certificazione
Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali	- La registrazione delle attivita' di trattamento e delle categorie di trattamenti viene effettuata a mezzo del Registro del titolare, in atti, e del Registro dei responsabili

SEZIONE II
VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD
(art. 35, paragrafo 7, lettera b)

A) NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.b)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'	- Finalita' determinate, esplicite e legittime: controlli e verifiche, anche a campione, che le finalita' del trattamento siano conformi al dettato normativo, risultino esplicitare e legittime - Principio di necessita' nel trattamento dei dati e dati personali adeguati, pertinenti e limitati a quanto necessario: controlli e verifiche, anche a campione, che i sistemi informativi e programmi informatici configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita' - Principio di correttezza e dati personali esatti e, se necessario, aggiornati: controlli e verifiche, anche a campione, su esattezza e aggiornamento dei dati

copia informatica per consultazione

	- Principio di limitazione della conservazione: controlli e verifiche, anche a campione, che i dati siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati
Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'	- Idonee misure volte a agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili - Idonee misure volte a: a) comunicare al richiedente i dati estratti a cura del responsabile o degli incaricati anche oralmente, ovvero a offrire tali dati in visione mediante strumenti elettronici, fermo restando che la comprensione dei dati deve essere agevole, considerata anche la qualita' e la quantita' delle informazioni b) a trasporre, se vi e' richiesta, i dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica - Idonee misure volte a garantire che, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprenda tutti i dati personali che riguardano l'interessato comunque trattati dal titolare - Idonee misure volte a prescrivere che, quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato possa avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti con correlata definizione dei criteri per l'identificazione degli atti e documenti - Idonee misure volte a semplificare le modalita' e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico - Idonee misure volte a garantire che la comunicazione dei dati sia effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile, fermo restando che, in caso di comunicazione di codici o sigle vanno forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato - Idonee misure volte a inserire il procedimento/processo, ad istanza di parte, relativo all'esercizio dei diritti degli interessati nel PTPC

A) CONFORMITA' RGPD

RGPD	FRAMEWORKS FUNZIONE
art.35 lett.d)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

copia informatica per consultazione

Misure previste per dimostrare la conformita' al RGPD	- Tracciabilita' documentale del processo decisionale di gestione del rischio

SEZIONE III
VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI
(art. 35, paragrafo 7, lettera c)

A) RISCHI

RGPD	**FRAMEWORKS FUNZIONE**
art.35 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
RISCHI **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati*** (rilevati dalla prospettiva degli interessati)	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura - OPERATORI: errore umano nella gestione del trattamento - CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali - OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati - OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati - OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati - CONTESTO: instabilita' rete elettrica per sbalzi di tensione - APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative

copia informatica per consultazione

	implementazioni) - APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione/alterazione credenziali di autenticazione - OPERATORI: accesso non autorizzato e/o uso improprio della rete internet - APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: elenco degli incaricati accessibile

copia informatica per consultazione

	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - CONTESTO: sottrazione strumenti contenenti dati - CONTESTO: sottrazione documenti cartacei - CONTESTO: ingressi non autorizzati ad aree e locali - CONTESTO: malfunzionamento sistemi di climatizzazione - APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - OPERATORI: accesso non autorizzato ai documenti cartacei - OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione - CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza - CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti - CONTESTO: assenza di istruzioni operative - CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC - OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-

copia informatica per consultazione

	mail ad un destinatario sbagliato - CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda - APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni) - APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)
RISCHI Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- Cancellazione di dati (i dati non sono piu' sui sistemi del titolare e non li ha neppure l'autore della violazione) - Alterazione di dati (i dati sono presenti sui sistemi ma sono stati alterati) - Furto di dati (i dati non sono piu' sui sistemi del titolare e li ha l'autore della violazione) - Copiatura di dati (i dati sono ancora presenti sui sistemi del titolare) - Lettura di dati (presumibilmente i dati non sono stati copiati)
Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati (rilevati dalla prospettiva degli interessati)	- CAUSA DI INCIDENTI: attacchi Denial of service - CAUSA DI INCIDENTI: cyber spionaggio - CAUSA DI INCIDENTI: violazione delle carte di pagamento - CAUSA DI INCIDENTI: sviluppo tecnologico che puo' produrre conseguenze pregiudizievoli - CAUSA DI INCIDENTI: intrusioni point-of-sale - CAUSA DI INCIDENTI: web app tracks
PROBABILITA' = X (rilevata dalla prospettiva degli interessati)	Medio
GRAVITA' = Y (rilevata dalla	Molto alto

copia informatica per consultazione

prospettiva degli interessati)	
STIMA (XxY) DELLA PROBABILITA' E GRAVITA' (rilevata dalla prospettiva degli interessati)	Molto alto

MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA

 Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:

 - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;
- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

 1 = basso-trascurabile = e' **molto improbabile** che la minaccia si possa verificare
 2 = medio = e' **improbabile** che la minaccia si possa verificare
 3 = alto = = e' **probabile** che la minaccia si possa verificare
 4 = molto alto = e' **altamente probabile** che la minaccia si possa verificare

 - IMPATTO, quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
 - livello dell'impatto, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).

 1 = basso-trascurabile
 2 = medio
 3 = alto
 4 = molto alto

 La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

Valore del rischio da 1 a 2 = RISCHIO BASSO (verde)
Valore del rischio da 3 a 4 = RISCHIO MEDIO (giallo)
Valore del rischio da 6 a 9 = RISCHIO ALTO (arancione)
Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO (rosso)

copia informatica per consultazione

MINACCE PROBABILITA' / IMPATTO GRAVITA'	1 bassa-trascurabile	2 media	3 alta	4 molto alta
1 basso-trascurabile	1	2	3	4
2 medio	2	4	6	8
3 alto	3	6	9	12
4 molto alto	4	8	12	16

La stima del rischio costituisce l'input per definire e selezionare:

- le politiche di sicurezza
- le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI

RGPD	FRAMEWORKS FUNZIONE	RISCHI CONTRASTATI
art.35 lett.c)	**Proteggere**	Come da MAPPA dei rischi contrastati
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**	
Misure di sicurezza: tecniche logistiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio	

copia informatica per consultazione

	della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Misure di sicurezza: tecniche informatiche, comprese le misure di ripristino in caso di data breach	- ABSC 01 (CSC 1) - inventario dei dispositivi autorizzati e non autorizzati: gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e

copia informatica per consultazione

	relative implementazioni effettuate dal titolare)
Misure di sicurezza: Organizzative	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Misure di sicurezza: procedurali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e

copia informatica per consultazione

	attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

C) RISCHIO RESIDUO

RGPD	**FRAMEWORKS FUNZIONE**
art.36 lett.c)	**Valutare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Livello rischio dopo l'applicazione delle misure	- Rischio residuo non elevato, e conseguente decisione di procedere con il trattamento con le misure di sicurezza in precedenza indicate

D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE

RGPD	**FRAMEWORKS FUNZIONE**
art.36	**Consultare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**

SEZIONE IV
DOCUMENTAZIONE
(art. 24, paragrafo 1)

RGPD	**FRAMEWORKS FUNZIONE**
art.24	**Documentare**
CRITERI LINEE	**DPIA TRATTAMENTO**

copia informatica per consultazione

GUIDA	
Documentare la conformita' al RGPD	- La conformita' giuridica al GDPR e' provata da: a) tutta la documentazione del sistema di protezione e, in particolare, dagli atti di delega e di nomina, dalle istruzioni operative e dalle clausole di garanzia e tutela inserite nei contratti di outsourcing; b) dai documenti di preliminare determinazione della possibilita' che il trattamento possa avere un rischio elevato nonche', in caso di rischio elevato, dai documenti di DPIA; c) dai registri delle attivita' e delle categorie di trattamento .

SEZIONE IV
MONITORAGGIO E RIESAME DPIA
(art. 35, paragrafo 11)

RGPD	FRAMEWORKS FUNZIONE
art. 35	**Monitorare**
CRITERI LINEE GUIDA	**DPIA TRATTAMENTO**
Stato attuazione misure	- Parzialmente attuate
Fasi attuazione misure	- Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1 - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3 - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2 - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4
Indicatori attuazione misure	- Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato
Responsabile attuazione misure	Soggetto individuato in base agli atti di organizzazione

RIESAME DPIA	
Motivazione riesame	- La valutazione e il presente documento sono soggetti a costante riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto

copia informatica per consultazione

**ELENCO DEI TRATTAMENTI
INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI**

Riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa
Assunzione personale appartenente a categorie protette (Legge 68/1999)

21

copia informatica per consultazione

AREA	SERVIZIO	SERVIZIO	Denominazione trattamento	Attivita'/processo oggetto del trattamento	Assoggettabilita' DPIA
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	Convenzioni tra i comuni e tra i comuni e provincia, costituzione e modificazione di forme associative	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Statuti dell'ente e delle aziende speciali, regolamenti nonche' criteri generali in materia di ordinamento degli uffici e dei servizi	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Programmazione e pianificazione	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Organismi di decentramento e di partecipazione - nomina	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	Modalita' di gestione dei pubblici servizi	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Istituzione e ordinamento dei tributi, con esclusione della determinazione delle relative aliquote; disciplina generale delle tariffe per la fruizione dei beni e dei servizi	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Indirizzi da osservare da parte delle aziende pubbliche e degli enti dipendenti, sovvenzionati o sottoposti a vigilanza	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Contrazione dei mutui non previsti espressamente in atti fondamentali del Consiglio Comunale ed emissione dei prestiti obbligazionari	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Spese che impegnano i bilanci per gli esercizi successivi, escluse quelle relative alle locazioni di immobili ed alla somministrazione e fornitura di beni e servizi a carattere continuativo	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Acquisti ed alienazioni immobiliari, relative permute, appalti e concessioni che non siano previsti espressamente in atti fondamentali del Consiglio o che non ne costituiscano mera esecuzione e che, comunque, non rientrino nella ordinaria amministrazione di funzioni e servizi di competenza della Giunta, del Segretario Generale o di altri funzionari	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Istituzione commissioni permanenti, temporanee o speciali	DPIA SI
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	Mozioni, ordini del giorno, risoluzioni, interrogazioni ed interpellanze	DPIA SI
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Parere sul documento delle linee programmatiche di mandato del Sindaco	DPIA NO
00 - AMMINISTRATORI	CONSIGLIO COMUNALE	Consiglio comunale e commissioni consiliari	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	Lasciti e donazioni	DPIA SI
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessioni discrezionali non vincolate di contributi, benefici, esoneri e sovvenzioni (Provvedimenti amministrativi discrezionali nell'an e nel contenuto)	DPIA SI
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Programmi, piani e progetti esecutivi attuativi del programma amministrativo del Sindaco, che non rientrano nella competenza del Consiglio comunale o nelle funzioni di gestione dell'Ente	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Atti di indirizzo e di amministrazione a contenuto generale	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Atti di controllo politico-amministrativo sui provvedimenti di gestione dell'Ente	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Regolamenti e bozze di atti fondamentali da sottoporre alle determinazioni del Consiglio e collaborazione nelle attivita' di iniziativa, d'impulso e di raccordo con gli organi di partecipazione	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Criteri generali per la determinazione delle tariffe	DPIA NO

copia informatica per consultazione

00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Indirizzi per la copertura dei posti della pianta organica	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Indirizzi, previa determinazione dei costi e individuazione dei mezzi, per l'esercizio delle funzioni conferite dalla Provincia, dalla Regione e dallo Stato	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Variazioni al bilancio ai sensi dell'articolo 42, comma 2, del T.U. 267/2000	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Indirizzi, criteri ed indicazioni per il conferimento di incarichi, consulenze, designazioni, nomine e composizioni di commissioni	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Indirizzi, criteri ed indicazioni per la concessione di contributi e sussidi non obbligatori a soggetti pubblici o privati	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Nomine e affidamenti incarichi per prestazioni o servizi per i quali le determinazioni siano fondate su rapporti fiduciari	DPIA SI
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Linee, misura delle risorse ed obiettivi da osservarsi dalla delegazione trattante di parte pubblica nella conduzione delle trattative per la contrattazione e per gli accordi decentrati, con autorizzazione preventiva alla sottoscrizione conclusiva dei contratti decentrati	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Assunzione di personale mediante concorsi, mobilita' e contratti di lavoro a tempo determinato o flessibile	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Indirizzi e criteri di massima per il nucleo di valutazione/OIV	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Esternalizzazione di attivita' comunali e servizi	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Misure tariffe, canoni, tasse ed oneri per le utenze dei servizi	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Indirizzi concernenti le condizioni e le clausole per gli accordi, le convenzioni, le concessioni, i contratti e le intese con soggetti pubblici e privati	DPIA NO
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Convenzioni con associazioni e altri enti di diritto privato non di competenza del Consiglio	DPIA SI
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	Convenzioni, transazioni ed ogni disposizione patrimoniale di straordinaria amministrazione	DPIA SI
00 - AMMINISTRATORI	GIUNTA COMUNALE	Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Indirizzi generali e obiettivi strategici in materia di prevenzione della corruzione e di trasparenza	DPIA NO
00 - AMMINISTRATORI	SINDACO	Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Attribuzione e revoca incarichi al personale dirigente	DPIA SI
00 - AMMINISTRATORI	SINDACO	Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Linee programmatiche di mandato	DPIA NO
00 - AMMINISTRATORI	SINDACO	Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Direttive e indirizzi in ordine al funzionamento e all'attivita' amministrativa	DPIA NO
00 - AMMINISTRATORI	SINDACO	Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Nomina e revoca assessori	DPIA SI
00 - AMMINISTRATORI	SINDACO	Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Nomina Segretario generale	DPIA SI
00 - AMMINISTRATORI	SINDACO	Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Nomina Organismo di valutazione	DPIA SI

copia informatica per consultazione

00 - AMMINISTRATORI	SINDACO	Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Coordinamento Assessori	DPIA NO
00 - AMMINISTRATORI	SINDACO	Sindaco	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	Ordinanze in qualita' di Ufficiale di governo	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Sistema di gestione del rischio di corruzione-PTPCT	DPIA NO
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	Gestione e archiviazione dei contratti pubblici	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	Accesso art. 43, co. 2 del T.U.E.L. da parte dei consiglieri	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	Accesso art. 22 e segg. della L. 241/90	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	Accesso art. 43, co. 2 del T.U.E.L. da parte dei consiglieri	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	Monitoraggio funzionamento PTPCT e monitoraggio singole misure	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	Autenticazione scritture private	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	Rogito atti segretario comunale	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	Trascrizione decreti esproprio e altri	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	Liquidazione diritti di segreteria	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	Registrazione contratti	DPIA SI
01 - SEGRETARIO COMUNALE	Segretario Comunale	Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	Adempimenti conseguenti alla stipula del contratto: registrazione anni successivi	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Registro convivenze di fatto	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Anagrafe: Iscrizioni registri anagrafici	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Anagrafe: Cancellazioni registri anagrafici per irreperibilita'	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Comunicazioni Prefettura	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Comunicazioni all'ufficio tributi	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Concessioni demaniali per tombe di famiglia	DPIA NO
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Tenuta registro unioni civili	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Accettazione e tenuta dichiarazioni di testamento biologico	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Acquisizione della cittadinanza italiana per riconoscimento o dichiarazione giudiziale della filiazione durante la minore eta' del figlio, o nel caso in cui la paternita' o maternita' non puo' essere dichiarata, purche' sia stato riconosciuto giudizialmente il diritto al mantenimento o agli alimenti, di minore straniero	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Acquisizione della cittadinanza italiana per riconoscimento o dichiarazione giudiziale della filiazione o nel caso in cui la paternita' o maternita' non puo' essere dichiarata, purche' sia stato riconosciuto giudizialmente il diritto al mantenimento o agli alimenti, di maggiorenne straniero	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Anagrafe: Adeguamento anagrafe ai risultati del censimento	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Toponomastica: Attribuzione numero civico	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Certificazioni anagrafiche	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Toponomastica: Denominazione nuove strade e piazze	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Variazioni anagrafiche AIRE (Anagrafe Italiani Residenti all'Estero)	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Iscrizione AIRE (Anagrafe Italiani Residenti all'Estero) dei cittadini italiani per trasferimento da AIRE o APR di altro Comune	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	Accertamento requisiti di dimora abituale delle variazioni di residenza	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Ripristino immigrazione	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Anagrafe: Variazione di indirizzo	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Verifica dichiarazione di rinnovo della dimora abituale	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Attestazione di regolarita' di soggiorno	DPIA SI

copia informatica per consultazione

02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Attestazione di soggiorno permanente	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Rilascio di documenti di identita'	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Autentica di firma	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Autentica di copia	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Cancellazione anagrafiche AIRE (Anagrafe Italiani Residenti all'Estero)	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Anagrafe: Certificati anagrafici storici	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Tutela/Curatela	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Trascrizione atti di nascita formati all'estero	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Trasmissioni alla Procura della Repubblica	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Comunicazioni all'Ufficio anagrafe	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Celebrazioni matrimoni e unioni civili	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Pubblicazioni di matrimonio	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Disconoscimenti	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Riconoscimenti	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Annotazione sentenza di rettificazione attribuzione di sesso	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Annotazione sentenze di scioglimento del matrimonio civile, di cessazione degli effetti civili del matrimonio religioso (concordatario) o di delibazione sentenze ecclesiastiche di annullamento di matrimonio pronunciate in Italia, provenienti da altri comuni	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Separazione consensuale, divorzio congiunto e modifica delle condizioni di separazione o di divorzio innanzi all'Ufficiale di Stato Civile	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato Civile: Trascrizione atto di matrimonio celebrato all'estero	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Adozione	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Trascrizione atti di nascita rese dalla Direzione Sanitaria	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Trascrizione atto di nascita neo-cittadino	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Trascrizione atto di matrimonio celebrato in altro comune italiano	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato Civile: Trascrizione atto di matrimonio concordatario	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	Gestione e dislocamento delle salme	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Redazione atto di morte	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Trascrizione atto di morte avvenuta all'estero	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Autorizzazione ai custodi ad effettuare l'inumazione delle salme	DPIA NO
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato civile: Trascrizione atto di morte pervenuto da altro Comune	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Stato Civile: Rilascio passaporto mortuario	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Autorizzazione alla tumulazione di salme/resti/ceneri nel loculo assegnato	DPIA NO
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Stato civile: Autorizzazione alla cremazione	DPIA NO
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Autorizzazione alla dispersione delle ceneri	DPIA NO
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	Elettorale: supporto commissioni elettorali	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	Leva: Variazioni liste di leva	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	Elettorale: autorizzazione al voto fuori sezione	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	Elettorale: voto domiciliare	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	Elettorale: voto assistito	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	Elettorale: rilascio tessera elettorale	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	Elettorale: revisione dinamica liste elettorali	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	Elettorale: iscrizione nell'albo degli scrutatori	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	Elettorale: aggiornamento Albo scrutatori	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	Elettorale: iscrizione nell'albo dei Presidenti di seggio	DPIA SI

copia informatica per consultazione

02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari	Elettorale: iscrizione nell'albo dei Giudici Popolari	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 09 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari	Elettorale: revisione semestrale liste elettorali	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)	Statistiche	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Atti di nascita, morte, cittadinanza e matrimonio	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	Pratiche anagrafiche	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	Gestione delle sepolture e dei loculi	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari	Consultazioni elettorali	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	Gestione dell'elettorato	DPIA SI
02 - Area Amministrativa	ANAGRAFE, STATO CIVILE, ELETTORALE, LEVA, STATISTICA E POLIZIA MORTUARIA	Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	Gestione della leva	DPIA SI
02 - Area Amministrativa	SERVIZI LEGALI	Servizi Legali	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione	Affidamento del contenzioso GdP e Tribunale alla difesa esterna mediante il sistema dell'affidamento diretto	DPIA SI
02 - Area Amministrativa	SERVIZI LEGALI	Servizi Legali	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Gestione dei procedimenti di segnalazione e reclamo	DPIA SI
02 - Area Amministrativa	SERVIZI LEGALI	Servizi Legali	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Supporto giuridico e pareri legali	DPIA SI
02 - Area Amministrativa	SERVIZI LEGALI	Servizi Legali	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione	Gestione del contenzioso	DPIA SI
02 - Area Amministrativa	SERVIZIO NOTIFICA	Servizio Notifica	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	Albo e notifiche: Notifiche	DPIA SI
02 - Area Amministrativa	SERVIZIO NOTIFICA	Servizio Notifica	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	Albo e inviti: Inviti consigli comunali	DPIA SI
02 - Area Amministrativa	SERVIZIO NOTIFICA	Servizio Notifica	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	Albo: Pubblicazioni albo on-line	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 23 - Istruzione e cultura - Trattamento di dati relativi alla gestione delle biblioteche e dei centri di documentazione	Servizi di gestione biblioteche	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 11 - Servizi sociali - Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale	Servizio di assistenza educativa alunni disabili in ambito scolastico	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Concessione prestazioni agevolate (servizi educativi, socio-assistenziali, etc.)	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Piano diritto allo studio	DPIA NO
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Servizio di ristorazione scolastica	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessione contributo a istituti scolastici paritari	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessione contributo regionale buono-libri	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Servizio di fornitura testi scolastici per alunni della scuola primaria	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Servizio pre e post scuola	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Servizio di trasporto scolastico	DPIA SI
02 - Area Amministrativa	SERVIZIO SCUOLA E BIBLIOTECA	Servizio Scuola e Biblioteca	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	Asili nido	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Portineria e custodia: Conservazione chiavi	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	Controllo strategico ai sensi dell'art. 147-ter del D.Lgs. 267/2000	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	Controllo successivo di regolarita' amministrativa e contabile ai sensi dell'art. 147-bis del D.Lgs. 267/2000	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	Centralino: Gestione del flusso delle telefonate	DPIA NO

copia informatica per consultazione

02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	Rilascio copia dei contratti stipulati con l'amministrazione	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Liquidazioni acconti o rata di saldo e omologa del certificato di regolare esecuzione per contratti pubblici di lavori, servizi e forniture in economia	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	Stampa giornaliera ed annuale del registro di protocollo informatico	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Gare ad evidenza pubblica di concessione di beni e servizi	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Partecipazione a coordinamenti intercomunali	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Convenzioni con associazioni di volontariato	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	Istruttoria delle deliberazioni	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	Denunce infortuni sul lavoro	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	Gestione dell'archivio storico	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Affidamento mediante procedura aperta (o ristretta) di lavori, servizi, forniture	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Affidamento diretto di lavori, servizi o forniture	Da valutare
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Proposta di aggiudicazione in base al prezzo	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Proposta di aggiudicazione in base all'OEPV	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Pulizia degli immobili e degli impianti di proprieta' dell'ente	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	Controllo - Ispezione	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	Comunicazioni di pubblica utilita'	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	Carte dei Servizi	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	Indagini di customer satisfaction e qualita'	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	Raccolta e distribuzione di modulistica relativa alle procedure di competenza degli Uffici	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	Raccolta, ritiro, catalogazione e distribuzione al pubblico di materiale informativo e divulgativo su servizi istituzionali comunali o di altri enti, su iniziative culturali e per il tempo libero	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	Gestione S.I. e rete: Creazione caselle di posta elettronica	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Designazione dei rappresentanti dell'ente presso enti, societa', fondazioni	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Nomina della commissione giudicatrice art. 77	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Pagamento premi e gestione polizze assicurative	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Registro dei responsabili del trattamento relativo alle attivita' di trattamento dei dati personali	DPIA SI

copia informatica per consultazione

02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Registro del titolare del trattamento dei dati personali	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Proroga contratto in scadenza	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Adesione convenzioni CONSIP o del Soggetto Aggregatore di riferimento	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Affidamento appalto di servizi e forniture di importo superiore alle soglie di cui all'art. 14, D.Lgs. 36/2023 attraverso il sistema della procedura aperta	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Affidamento appalto di servizi e forniture di importo pari o superiore a 140.000 euro e inferiore alle soglie di cui all'articolo 14, D.Lgs. 36/2023 mediante il sistema della procedura negoziata	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	Segnalazione-Esposto	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	Segnalazioni di illecito	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	Autorizzazione al ricorso a transazioni e altri rimedi di risoluzione delle controversie alternativi a quelli giurisdizionali	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	Accesso civico semplice concernente dati, documenti e informazioni soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	Accesso civico generalizzato concernente dati e documenti ulteriori a quelli soggetti a pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	Registro degli accessi	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	Front office: Informazioni e comunicazioni	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Agenda Sindaco ed Assessori	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	Ricevimento pubblico	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Gestione sedute commissioni consiliari	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Gestione sedute conferenze capigruppo	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Gestione sedute Consiglio comunale	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Selezione per l'affidamento di incarichi professionali	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Trascrizione verbali consiglio	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Surroghe	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Convalida consiglieri	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Funzionamento degli organi collegiali	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Nomina Presidente e vicepresidenti	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Decadenze	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Fornitura servizi ai gruppi consiliari	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Assistenza organi istituzionali: Gestione sedute Giunta comunale	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	Verifica delle offerte anomale art. 97	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	Anagrafe degli eletti: Pubblicazione e aggiornamento dati on line	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA DEL SINDACO E RELAZIONI ESTERNE	Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Concessione sala Consiliare	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA E PROTOCOLLO	Servizio Segreteria e Protocollo	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	Pubblicazione delle deliberazioni	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA E PROTOCOLLO	Servizio Segreteria e Protocollo	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	Gestione del protocollo	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA E PROTOCOLLO	Servizio Segreteria e Protocollo	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	Gestione dell'archivio corrente e di deposito	DPIA SI

copia informatica per consultazione

02 - Area Amministrativa	SERVIZIO SEGRETERIA E PROTOCOLLO	Servizio Segreteria e Protocollo	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	Gestione del sito web	DPIA NO
02 - Area Amministrativa	SERVIZIO SEGRETERIA E PROTOCOLLO	Servizio Segreteria e Protocollo	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	Servizi di disaster recovery e backup	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA E PROTOCOLLO	Servizio Segreteria e Protocollo	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	Servizi di gestione hardware e software	DPIA SI
02 - Area Amministrativa	SERVIZIO SEGRETERIA E PROTOCOLLO	Servizio Segreteria e Protocollo	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	Assistenza utenti: Interventi supporto per la gestione dati applicativi	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Contrassegni	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	Servizio trasporto extraurbano minori e disabili	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	Servizio trasporto urbano minori e disabili	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	Gestione degli alloggi pubblici	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	Servizi per minori e famiglie	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio	Servizio centro ricreativo estivo - CRE	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Concessione buono casa	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Concessione buono elettricista	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	Servizi per adulti in difficolta'	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Servizio di controllo I.S.E.E. per prestazioni sociali agevolate	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Servizio accreditamenti servizi socio-assistenziali	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	Rilascio di patrocini	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessione di sovvenzioni, contributi, sussidi, ecc.	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	Organizzazione eventi culturali ricreativi	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Servizi di gestione musei	DPIA NO
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	Servizi di gestione impianti sportivi	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessione di premi in occasione di manifestazioni sportive	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessione contributi per manifestazioni	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessione contributi ad associazioni sportive dilettantistiche	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessione tariffe agevolate	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	Concessione contributi ordinari in denaro a sostegno dell'attivita' ordinaria del privato, dell'ente o dell'associazione richiedente	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Servizio di gestione tariffe e rette	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	Gestione sito web: Creazione pagine	DPIA NO

copia informatica per consultazione

02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	Gestione sito web: Software per la gestione dei contenuti	DPIA NO
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	Liquidazione fatture	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	Concessione integrazione rette case di riposo	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	Servizio RSA e riabilitazione	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Concessione contributi economici	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Concessione contributi per badanti	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Concessione Carta per ottenere agevolazioni presso gli esercizi commerciali	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 15 - Servizi sociali - Trattamento di dati relativi all'attivita' di gestione dell'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	Servizi assistenziali e socio-sanitari per anziani	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	Servizio di trasporto anziani	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	Procedure correlate alla nomina amministratore di sostegno, interdizione o inabilitazione (su richiesta dell'autorita' giudiziaria)	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Convenzioni con Centri di socializzazione	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare	Servizio assistenza domiciliare minori	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	Servizi per disabili	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	Servizio ricovero minori in struttura	DPIA SI
02 - Area Amministrativa	SERVIZIO SOCIO CULTURALE, SPORT E VOLONTARIATO	Servizio Socio Culturale, Sport e Volontariato	Scheda n. 55 - Servizi Sociali - Trattamento di dati relativi all'attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al "Sistema di protezione dei richiedenti asilo e rifugiati"	Servizi di integrazione dei cittadini stranieri	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Incentivi economici al personale (produttivita' e retribuzioni di risultato)	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Contrattazione decentrata integrativa	DPIA NO
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Servizi di formazione del personale dipendente	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Sorveglianza sanitaria a cura del medico competente	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Conferimento di incarichi di collaborazione, studio e ricerca nonche' di consulenza a soggetti estranei all'amministrazione	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Pensioni: Pratiche	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Rilascio certificato di stipendio	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Statistiche	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Rimborso oneri per datore di lavoro	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	Riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Programma triennale ed annuale del fabbisogno di personale	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Concorso per l'assunzione di personale	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Selezioni da centro per l'impiego	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Stabilizzazioni	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Mobilita' dall'esterno ex art. 30 del D.Lgs. 165/2001	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Mobilita' ex art. 34 bis, D.Lgs. 165/2001	DPIA SI

copia informatica per consultazione

02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Mobilita' interna intersettoriale da P.E.G.	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Cambi di profilo professionale	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Trasformazione del rapporto di lavoro a tempo parziale	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Denunce infortuni sul lavoro	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Medico competente - nomina	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Assistenza attivita' di valutazione della performance e assegnazione punteggi e premi degli OIV/Nuclei	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Gestione coperture INAIL	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Comandi e trasferimenti	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Nomina componenti del CUG	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Nomina componenti del Nucleo di valutazione - OIV	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Rilevazione eccedenze personale	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Assunzioni interinali	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Attribuzione incarichi dirigenziali	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Certificazioni e attestazioni posizioni assicurative (pa) per uso ricongiunzioni, riscatti ed altro	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Certificazioni stipendio per cessione quinto - prestiti e cessioni	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Concorso per la progressione in carriera del personale	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	Assunzione personale appartenente a categorie protette (Legge 68/1999)	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Gestione giuridica del personale: permessi, ferie, ecc.	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Relazioni sindacali (informazione, ecc.)	DPIA SI
02 - Area Amministrativa	UFFICIO PERSONALE	Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Sorveglianza sanitaria D. Lgs. 81/2008 - planning visite e certificazioni di idoneita' al lavoro	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizi Finanziari	Servizi Finanziari	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Gestione ordinaria delle spese di bilancio	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizi Finanziari	Servizi Finanziari	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Gestione ordinaria della entrate	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizi Finanziari	Servizi Finanziari	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Adempimenti fiscali	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Attivita' Economiche S.U.A.P.	Servizio Attivita' Economiche	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Autorizzazione all'occupazione del suolo pubblico	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Nessun trattamento - Assenza dati personali da trattare	Controllo sulle societa' partecipate	Assenza di dati personali da trattare
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Nessun trattamento - Assenza dati personali da trattare	Tenuta ed aggiornamento dell'archivio relativo alle societa' nonche' delle aziende speciali ed altri enti pubblici partecipati dall'Ente (Enti controllati)	Assenza di dati personali da trattare
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Nessun trattamento - Assenza dati personali da trattare	Invio dell'elenco delle societa' partecipate al Dipartimento della Funzione Pubblica	Assenza di dati personali da trattare
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Nessun trattamento - Assenza dati personali da trattare	Predisposizione di certificazioni, rendiconti e statistiche riguardanti le societa' partecipate (Enti controllati)	Assenza di dati personali da trattare
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Nessun trattamento - Assenza dati personali da trattare	Procedure di dismissione di partecipazioni azionarie ed altre quote societarie	Assenza di dati personali da trattare
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Bilancio di previsione	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Certificazioni del bilancio preventivo e consuntivo ed altre certificazioni	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Controllo equilibri finanziari	DPIA NO

copia informatica per consultazione

03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Documento Unico di Programmazione - DUP	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Inserimento e controllo dati IVA	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Inventario beni mobili.	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Mandati di pagamento	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Parere di regolarita' contabile	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Parere sugli atti con finanziamenti in conto capitale	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Piano esecutivo di gestione - PEG	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Recupero e registrazione giornaliera delle operazioni del Tesoriere relative ai versamenti in Tesoreria da parte degli utenti e chiusura mensile dei sospesi del Tesoriere	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Rendiconto	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Variazioni al bilancio di previsione e P.E.G.	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	Verifiche Revisore dei Conti	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Versamenti addizionale comunale rateizzata	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Bilancio	Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	Versamenti addizionale regionale rateizzata	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Economato	Servizio Economato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Fornitura cancelleria ed altro materiale di consumo per gli uffici	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Economato	Servizio Economato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Consegna arredi e attrezzature uffici	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Economato	Servizio Economato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Consegne materiali	DPIA NO
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	Accertamenti e verifiche dei tributi locali	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	Controllo tassa sui rifiuti TARES/TARI	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	Rateazione pagamento tributi accertati	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	Servizio rilascio certificati relativi a posizioni tributarie	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	Provvedimenti in autotutela per tributi comunali	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	Servizio informativo risposte a istanze, comunicazioni, richieste di informazioni opposizioni	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	Rimborsi a contribuenti - riversamenti a Comuni competenti - sgravi di quote indebite e inesigibili di tributi comunali	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	Istanze interpello	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Servizio Tributi	Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	Accertamenti con adesione dei tributi locali	DPIA SI
03 - AREA FINANZIARIA - TRIBUTARIA	Ufficio Gestione economica Personale	Ufficio Gestione economica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Stipendi e Paghe	DPIA SI
04 - Area tecnica Edilizia e Urbanistica	Servizio Demanio	Servizio Demanio	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Assistenza e manutenzione in occasione di manifestazioni	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Demanio	Servizio Demanio	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Rilascio concessioni demaniali	DPIA NO

copia informatica per consultazione

04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Costruzione in area di rispetto del demanio marittimo - Autorizzazione e attivita' edilizia libera	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Costruzioni in area di rispetto del demanio marittimo - CILA SCIA piu' autorizzazione (la mappatura si riferisce alla CILA)	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Costruzione in area di rispetto del demanio marittimo - Autorizzazione PdC piu' Autorizzazione.	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Costruzioni o opere in prossimita' della linea doganale in mare territoriale - CILA/SCIA piu' autorizzazione (la mappatura si riferisce alla CILA)	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Permesso di costruire	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Permesso di costruire in aree assoggettate ad autorizzazione paesaggistica	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Permesso di costruire convenzionato	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Autorizzazioni Paesaggistiche	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	SCIA, CILA, CIL	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Edilizia	Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	Provvedimenti sanzionatori (ordinanze pagamento/Ordinanze di demolizione)	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Urbanistica	Servizio Urbanistica	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Provvedimenti di pianificazione urbanistica generale	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Urbanistica	Servizio Urbanistica	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Gestione del reticolo idrico minore	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Urbanistica	Servizio Urbanistica	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Provvedimenti di pianificazione urbanistica attuativa	DPIA NO
04 - Area tecnica Edilizia e Urbanistica	Servizio Urbanistica	Servizio Urbanistica	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Procedimento per l'insediamento di una nuova cava	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	Piano delle alienazioni e valorizzazioni	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	Assegnazione Alloggi Edilizia Residenziale Pubblica - E.R.P.	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Concessione a titolo gratuito delle sale e immobili del patrimonio comunale	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	Accertamento requisiti di dimora abituale delle variazioni di residenza	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Vendita beni patrimonio disponibile mediante asta pubblica	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Servizio di gestione canoni demaniali	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Procedure di accatastamento immobili	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Registrazione movimenti inventariali	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Concessioni canali demaniali irrigui	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Rimborso spese utenze immobili in locazione	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Locazione immobili urbani	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Nessun trattamento - Assenza dati personali da trattare	Pareri congruita' canoni locazioni passive	Assenza di dati personali da trattare
05 - Area tecnica Lavori Pubblici e Ambiente	Gestione Patrimonio Immobiliare	Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Servizio di custodia e sorveglianza immobili	DPIA NO

copia informatica per consultazione

05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Ambiente e Infrastrutture	Servizio Ambiente e Infrastrutture	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Installazione e manutenzione segnaletica, orizzontale e verticale, su strade e aree pubbliche	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Ambiente e Infrastrutture	Servizio Ambiente e Infrastrutture	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	Tributi locali (IMU, addizionale IRPEF, ecc.)	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Ambiente e Infrastrutture	Servizio Ambiente e Infrastrutture	Scheda n. 52 - Ufficio Ambiente - Trattamento di dati relativi all'attivita' di gestione dei rifiuti	Raccolta, recupero e smaltimento rifiuti	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Ambiente e Infrastrutture	Servizio Ambiente e Infrastrutture	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	Gestione delle Isole ecologiche	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Ambiente e Infrastrutture	Servizio Ambiente e Infrastrutture	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Manutenzione delle strade e delle aree pubbliche	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Ambiente e Infrastrutture	Servizio Ambiente e Infrastrutture	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Pulizia delle strade e delle aree pubbliche	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Manutenzione degli immobili e degli impianti di proprieta' dell'ente	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Procedimenti di esumazione ed estumulazione	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Programmazione dei lavori art. 21	Da valutare
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	Programmazione di forniture e di servizi	Da valutare
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Manutenzione dei cimiteri	DPIA SI
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Servizi di custodia dei cimiteri	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Manutenzione degli edifici scolastici	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	Servizi di pubblica illuminazione	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Manutenzione della rete e degli impianti di pubblica illuminazione	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Pulizia dei cimiteri	DPIA NO
05 - Area tecnica Lavori Pubblici e Ambiente	Servizio Lavori pubblici	Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	Manutenzione delle aree verdi	DPIA NO
06 - Area di Vigilanza	Servizio di Protezione Civile	Servizio di Protezione Civile	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	Servizi di protezione civile	DPIA SI
06 - Area di Vigilanza	Servizio Polizia amministrativa	Servizio Polizia Ammistrativa	Scheda n. 29 - Trattamento di dati relativi al rilascio delle licenze e autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza	Autorizzazioni ex artt. 68 e 69 del TULPS (spettacoli, intrattenimenti, ecc.)	Da valutare
06 - Area di Vigilanza	Servizio Polizia amministrativa	Servizio Polizia Ammistrativa	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	Vigilanza e verifiche su mercati ed ambulanti	DPIA SI
06 - Area di Vigilanza	Servizio Polizia amministrativa	Servizio Polizia Ammistrativa	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	Accertamenti e controlli sull'attivita' edilizia privata (abusi)	DPIA SI
06 - Area di Vigilanza	Servizio Polizia amministrativa	Servizio Polizia Ammistrativa	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	Controlli sull'uso del territorio	DPIA SI
06 - Area di Vigilanza	Servizio Polizia amministrativa	Servizio Polizia Ammistrativa	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	Controlli sull'abbandono di rifiuti urbani	DPIA SI
06 - Area di Vigilanza	Servizio polizia urbana	Servizio Polizia Urbana	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	Gestione delle sanzioni per violazione del Codice della strada	DPIA SI
06 - Area di Vigilanza	Servizio polizia urbana	Servizio Polizia Urbana	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	Sicurezza ed ordine pubblico	DPIA SI
06 - Area di Vigilanza	Servizio polizia urbana	Servizio Polizia Urbana	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	Vigilanza sulla circolazione e la sosta	DPIA SI
06 - Area di Vigilanza	Servizio polizia urbana	Servizio Polizia Urbana	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	Vigilanza e verifiche sulle attivita' commerciali in sede fissa	DPIA SI
07 - Attivita' Trasversali	Attivita' Trasversali	Attivita' Trasversali	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	Formazione di determinazioni, ordinanze, decreti ed altri atti amministrativi	DPIA SI

copia informatica per consultazione

Descrizione dei luoghi	Accesso al pubblico	Chiusura	Registrazione degli accessi	Finestre con inferiate	Allarme	Sistema antincendio	Cassaforte	Altre caratteristiche
Palazzo Comunale Municipio PIAZZA DANTE ALIGHIERI, 1 - Campo nell'Elba SEDE DEL COMUNE	portone di legno con chiusura a chiave su piazza Dante- accesso secondario su via Verdi con cancello e porta antipanico	a chiave	NO	NO	NO	SI (ESTINTORE)	SI	
N. 2 Uffici Polizia Municipale accesso da Via Giuseppe Verdi - Campo nell'Elba	due porte finestre, previa ingresso con cancello su Via Verdi	a chiave- cancello con chiusura elettrica	NO	NO	NO	SI (ESTINTORE)	SI	
Archivio (Ex Scuola Elementare Frazione di Seccheto Via Provinciale snc)	NON previsto accesso al pubblico - Porta	a chiave	NO	NO	NO	SI (ESTINTORE)	NO	
Sede Protezione Civile (Loc. La Pila, Via Giovanni XXIII snc)	NON previsto accesso al pubblico - Porta finestra con persiane	a chiave	NO	NO	NO	SI (ESTINTORE)	NO	

copia informatica per consultazione

Nr. locale	Uffici	Ubicazione uffici	Descrizione uffici e contenuto
30	Area Finanziaria e Tributaria -Responsabile	Piazza Dante Alighieri, 1	Armadi chiusi con chiave: 1; Scaffalature: 1
29	Area Finanziaria e Tributaria -Economato	Piazza Dante Alighieri, 1	PC: 2; Cassaforte: 1; Armadi chiusi con chiave: 2 con alcune ante aperte; Mobile basso chiuso: 2
28	Area Tecnica Edilizia e Urbanistica	Piazza Dante Alighieri, 1	PC: 1; Armadi chiusi con chiave: 1 con alcune ante a vetro
27	Area Tecnica Edilizia e Urbanistica	Piazza Dante Alighieri, 1	PC: 2; Armadi chiusi con chiave: 2 di cui 1 con vetrate; Mobile basso chiuso: 1; Scaffalature: 1
26	Area Tecnica Edilizia e Urbanistica -Responsabile	Piazza Dante Alighieri, 1	PC: 1; Armadi chiusi con chiave: 1 con alcune ante a vetro;
25	Area Tecnica LL.PP. Ambiente	Piazza Dante Alighieri, 1	PC: 2; Armadi chiusi con chiave: 2; Mobile basso chiuso: 2
22	Area Tecnica LL.PP. Ambiente	Piazza Dante Alighieri, 1	PC: 1; Armadi chiusi con chiave: 2 di cui 1 con vetrate
24	Area Tecnica LL.PP. Ambiente	Piazza Dante Alighieri, 1	PC: 2; Armadi chiusi con chiave: 2 entrambi con vetrate; Mobile basso chiuso: 1
23	Area Tecnica LL.PP. Ambiente - Responsabile	Piazza Dante Alighieri, 1	PC: 1; Armadi chiusi con chiave: 2 di cui 1 con vetrate; Mobile basso chiuso: 1
21	Corridoio Area Tecnica	Piazza Dante Alighieri, 1	Stampanti: 1; Armadi chiusi con chiave: 1
31	Area Finanziaria e Tributaria	Piazza Dante Alighieri, 1	PC: 2; Stampanti: 1; Mobile basso aperto: 2
20	Segretario Generale	Piazza Dante Alighieri, 1	PC: 1; Stampanti: 1; Armadi chiusi con chiave: 3 di cui 1 con ante a vetro non chiuse; Mobile basso chiuso: 1
19	Area Amministrativa- Servizio notifica	Piazza Dante Alighieri, 1	PC: 1; Mobile basso chiuso: 1
18	Sala Consiliare	Piazza Dante Alighieri, 1	Armadi chiusi con chiave: 1 con vetrate
17	Area Amministrativa- Segreteria Sindaco	Piazza Dante Alighieri, 1	PC: 2; Stampanti: 1; Armadi chiusi con chiave: 3 di cui 2 con alcune ante a vetrata senza chiave
16	Sindaco	Piazza Dante Alighieri, 1	PC: 1; Armadi chiusi con chiave: 1 con vetrate; Mobile basso aperto: 2
15	Area Amministrativa- Segreteria Sindaco	Piazza Dante Alighieri, 1	PC: 1; Armadi chiusi con chiave: 1 con vetrate; Armadi con ante senza chiave: 1
14	Sala Giunta	Piazza Dante Alighieri, 1	PC: 1; Armadi chiusi con chiave: 2 con alcune ante a vetrate senza chiave; Scaffalature: 1
13	Area Amministrativa- Scuola	Piazza Dante Alighieri, 1	PC: 1; Armadi con ante senza chiave: 2; Mobile basso chiuso: 1
12	Androne Primo Piano	Piazza Dante Alighieri, 1	Stampanti: 1
1	Androne Piano Terra	Piazza Dante Alighieri, 1	Stampanti: 1
5	Stanza Server	Piazza Dante Alighieri, 1	PC: 1 pc server sistema informativo comunale + server NAS impianto sistema videosorveglianza
2	Area Amministrativa- Anagrafe	Piazza Dante Alighieri, 1	PC: 4; Stampanti: 4; Cassaforte: 2; Armadi chiusi con chiave: 4; Mobile basso chiuso: 3
11	Area Amministrativa- Protocollo	Piazza Dante Alighieri, 1	PC: 2; Armadi chiusi con chiave: 2; Mobile basso chiuso: 3
10	Area Finanziaria e Tributaria -Tributi	Piazza Dante Alighieri, 1	PC: 3; Armadi chiusi con chiave: 3; Mobile basso chiuso: 3
8	Area Finanziaria e Tributaria -SUAP	Piazza Dante Alighieri, 1	PC: 2; Armadi chiusi con chiave: 1; Mobile basso chiuso: 2; Scaffalature: 1
100	Area di Vigilanza- Responsabile	Piazza Dante Alighieri, 1	PC: 1; Armadi chiusi con chiave: 1 con alcune ante a vetro
6 E 7	Area di Vigilanza- Polizia Municipale	Piazza Dante Alighieri, 1	PC: 4; Stampanti: 1; Cassaforte: 2; Armadi chiusi con chiave: 5; Scaffalature: 1
4	Ripostiglio mobile mensa	Piazza Dante Alighieri, 1	
30	Ufficio Mobile Polizia Municipale	Piazza Dante Alighieri, 1	Notebook: 2

copia informatica per consultazione

ID strumento	Nome Computer	Tipo di supporto	Sistema Operativo	Nr. locale	Nr. Locale (inventario)	Ubicazione	Scheda di rete	Connessione a rete locale	Software installato	Soggetti autorizzati all'accesso
2521	PC-SEG02	PC desktop	Windows 10 Pro	Area Amministrativa- Segreteria Sindaco	17	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2520	PC-SEG01	PC desktop	Windows 10 Pro	Area Amministrativa- Segreteria Sindaco	15	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2522	PC-SEG03	PC desktop	Windows 10 Pro	Area Amministrativa- Segreteria Sindaco	17	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2356	PC-SEG06	PC desktop	Windows 10 Pro	Area Amministrativa- Scuola	13	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2427	PC-Sindaco	PC desktop	Windows 10 Pro	Sindaco	16	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2326	PC-SCU02	PC desktop	Windows 10 Pro	Area Amministrativa- Servizio notifica	19	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2523	PC-segretario	PC desktop	Windows 10 Pro	Segretario Generale	20	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2639	PC-RAG02.campoelba.locale	PC desktop	Window 11 Pro	Area Finanziaria e Tributaria	31	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop, IRIS WIN	Dipendente assegnato all'Ufficio
2524	PC-TEC02	PC desktop	Windows 10 Pro	Area Tecnica LL.PP. Ambiente	22	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2525	PC-TEC01	PC desktop	Windows 10 Pro	Area Tecnica LL.PP. Ambiente - Responsabile	23	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2625	PC-TEC12	PC desktop	Windows 10 Pro	Area Tecnica LL.PP. Ambiente	24	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2527	PC-TEC10	PC desktop	Windows 10 Pro	Area Tecnica LL.PP. Ambiente	24	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2528	PC-TEC08	PC desktop	Windows 10 Pro	Area Tecnica LL.PP. Ambiente	25	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
*	PC-TEC11	PC desktop	Windows 10 Pro	Area Tecnica LL.PP. Ambiente	25	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2530	PC-TEC03	PC desktop	Windows 10 Pro	Area Tecnica Edilizia e Urbanistica -Responsabile	26	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2529	PC-TEC06	PC desktop	Window 11 Pro	Area Tecnica Edilizia e Urbanistica	27	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2393	PC-TEC09	PC desktop	Window 11 Pro	Area Tecnica Edilizia e Urbanistica	27	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
*	PC-TEC04	PC desktop	Window 11 Pro	Area Tecnica Edilizia e Urbanistica	28	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2531	PC-RAG05	PC desktop	Window 11 Pro	Area Finanziaria e Tributaria -Economato	29	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2532	PC-RAG04	PC desktop	Windows 10 Pro	Area Finanziaria e Tributaria -Economato	29	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop, IRIS WIN	Dipendente assegnato all'Ufficio
2533	PC-RAG01	PC desktop	Windows 10 Pro	Area Finanziaria e Tributaria -Responsabile	30	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2519	PC-PRO01	PC desktop	Windows 10 Pro	Area Amministrativa- Protocollo	11	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2518	PC-SEG04	PC desktop	Windows 10 Pro	Area Amministrativa- Protocollo	11	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2677	PC-Tri03	PC desktop	Windows 10 Pro	Area Finanziaria e Tributaria -Tributi	10	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2517	PC-TRI01	PC desktop	Windows 10 Pro	Area Finanziaria e Tributaria -Tributi	10	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2452	PC-TRI02	PC desktop	Windows 10 Pro	Area Finanziaria e Tributaria -Tributi	10	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2516	PC-COM02	PC desktop	Windows 10 Pro	Area Finanziaria e Tributaria -SUAP	8	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2517	PC-COM01	PC desktop	Windows 10 Pro	Area Finanziaria e Tributaria -SUAP	8	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2511	PC-ANA03	PC desktop	Windows 10 Pro	Area Amministrativa- Anagrafe	2	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2510	PC-ANA02	PC desktop	Windows 10 Pro	Area Amministrativa- Anagrafe	2	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2512	PC-VIG01	PC desktop	Windows 10 Pro	Area di Vigilanza- Responsabile	100	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2514	PC VIG12	PC desktop	Windows 10 Pro	Area di Vigilanza- Polizia Municipale	6 e 7	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2546	PC VIG09	PC desktop	Windows 10 Pro	Area di Vigilanza- Polizia Municipale	6 e 7	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	desktop, Drive Pro Body Toolbox,	Dipendente assegnato all'Ufficio
2513	PC VIG02	PC desktop	Windows 11 Pro	Area di Vigilanza- Polizia Municipale	6 e 7	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
_171	PC VIG05	PC desktop	Windows 7 professional	Area di Vigilanza- Polizia Municipale	6 e 7	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
2242	PC VIG08	PC desktop	Windows 7 professional	Area di Vigilanza- Polizia Municipale	6 e 7	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it	Pacchetto office, Adobe reader, GoSign desktop	Dipendente assegnato all'Ufficio
*		PC desktop		Area di Vigilanza- Polizia Municipale	6 e 7	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dor		Dipendente assegnato all'Ufficio
*		PC desktop		Area di Vigilanza- Polizia Municipale	6 e 7	Piazza Dante Alighieri, 1	SI	Il dominio della rete interna è campoelba.locale, il dominio della rete internet Se si riferiscono al dominio che il comune ha registrato per il sito internet è comune.campanellelba.li.it		Dipendente assegnato all'Ufficio

copia informatica per consultazione

SERVIZIO	Rischi	Gravità stimata	Motivazione stimata
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Attivita' Trasversali	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Attivita' Trasversali	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Attivita' Trasversali	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Attivita' Trasversali	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Attivita' Trasversali	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Attivita' Trasversali	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Attivita' Trasversali	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Attivita' Trasversali	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Attivita' Trasversali	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Consiglio comunale e commissioni consiliari	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Consiglio comunale e commissioni consiliari	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Consiglio comunale e commissioni consiliari	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Gestione Patrimonio Immobiliare	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Gestione Patrimonio Immobiliare	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati

copia informatica per consultazione

Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Gestione Patrimonio Immobiliare	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Giunta comunale	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Giunta comunale	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Giunta comunale	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Giunta comunale	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Giunta comunale	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Giunta comunale	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Giunta comunale	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Giunta comunale	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Giunta comunale	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Giunta comunale	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Giunta comunale	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Segretario Comunale	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Segretario Comunale	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Segretario Comunale	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Segretario Comunale	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Segretario Comunale	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Segretario Comunale	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Segretario Comunale	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Segretario Comunale	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Segretario Comunale	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Segretario Comunale	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizi Finanziari	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizi Finanziari	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizi Finanziari	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi

copia informatica per consultazione

Servizi Finanziari	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizi Finanziari	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizi Finanziari	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizi Finanziari	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Finanziari	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Finanziari	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizi Legali	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Servizi Legali	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizi Legali	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizi Legali	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizi Legali	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizi Legali	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizi Legali	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizi Legali	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Servizi Legali	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizi Legali	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizi Legali	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Ambiente e Infrastrutture	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Ambiente e Infrastrutture	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati

copia informatica per consultazione

Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Ambiente e Infrastrutture	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Attivita' Economiche	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Attivita' Economiche	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Attivita' Economiche	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Attivita' Economiche	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Attivita' Economiche	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Bilancio	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Bilancio	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Bilancio	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Bilancio	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Bilancio	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Bilancio	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Bilancio	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Bilancio	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Bilancio	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Bilancio	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Demanio	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Demanio	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Demanio	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi

copia informatica per consultazione

Servizio Demanio	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Demanio	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Demanio	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Demanio	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Demanio	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Demanio	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio di Protezione Civile	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Servizio di Protezione Civile	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio di Protezione Civile	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Servizio di Protezione Civile	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio di Protezione Civile	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Economato	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Economato	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Economato	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Economato	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Economato	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati

copia informatica per consultazione

Servizio Economato	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Economato	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Economato	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Economato	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Edilizia	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Edilizia	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Edilizia	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Edilizia	- APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Edilizia	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Lavori Pubblici	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati

copia informatica per consultazione

Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Lavori Pubblici	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Servizio Lavori Pubblici	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Lavori Pubblici	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Notifica	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Notifica	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Notifica	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Notifica	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Notifica	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Notifica	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Notifica	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Notifica	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Notifica	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Notifica	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Polizia Ammistrativa	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Polizia Ammistrativa	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Ammistrativa	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Polizia Urbana	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Servizio Polizia Urbana	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Polizia Urbana	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Polizia Urbana	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Polizia Urbana	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Scuola e Biblioteca	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Scuola e Biblioteca	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Scuola e Biblioteca	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Segreteria e Protocollo	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati

copia informatica per consultazione

Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Segreteria e Protocollo	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Servizio Segreteria e Protocollo	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria e Protocollo	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Segreteria Sindaco e Relazioni Esterne	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Socio Culturale, Sport e Volontariato	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Tributi	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Servizio Tributi	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Tributi	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Tributi	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Tributi	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Tributi	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Tributi	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Tributi	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Tributi	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Tributi	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Tributi	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Servizio Urbanistica	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: attacchi informatici/azione di virus/codici maligni	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Servizio Urbanistica	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Servizio Urbanistica	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Servizio Urbanistica	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Servizio Urbanistica	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Servizio Urbanistica	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Servizio Urbanistica	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Servizio Urbanistica	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Servizio Urbanistica	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Sindaco	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati

copia informatica per consultazione

Sindaco	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Sindaco	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Sindaco	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Sindaco	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Sindaco	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Sindaco	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

Sindaco	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Sindaco	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Sindaco	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Ufficio Gestione economica del personale dipendente	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Ufficio Gestione economica del personale dipendente	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio Gestione economica del personale dipendente	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: accesso non autorizzato ai locali per omessa sicurezza della struttura	Medio bassa	- L'accesso non autorizzato ai locali per omessa sicurezza della struttura non equivale, in automatico, a lesione dei dati
Ufficio gestione giuridica del personale dipendente	- OPERATORI: errore umano nella gestione del trattamento	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: incidenti o eventi avversi, come incendi o altre calamita' naturali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- OPERATORI: comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- OPERATORI: errore umano nella gestione delle apparecchiature o nei software che minacciano l'integrita' dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- OPERATORI: omesso controllo sul funzionamento dei back up e conseguente impossibilita' di ripristino dei dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: instabilita' rete elettrica per sbalzi di tensione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: accessi non autorizzati ai software e relativi archivi/banche dati con violazione misure minime ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: mancata protezione crittografica dei dati, presenza di dati rilevanti in chiaro, assenza di blacklist e/o assenza inadeguatezza di sistematica e efficace protezione dei dati con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: malfunzionamento per mancanza interventi di manutenzione sulla vulnerabilita' con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- Il malfunzionamento per mancanza di manutenzione non equivale in automatico a violazione dei dati
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: accessi a dispositivi elettronici non autorizzati e non gestiti con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: intercettazioni di informazioni gestite in rete con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: sottrazione/alterazione credenziali di autenticazione	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- OPERATORI: accesso non autorizzato e/o uso improprio della rete internet	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: assenza inventario in cui vengano elencati tutti gli identificativi e utenze amministrative scaduti o assegnati a incaricati esonerati dal servizio con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di black list in cui vengano elencati tutti gli identificativi scaduti o assegnati a incaricati esonerati dal servizio non osta a che l'obiettivo di identificazione sia realizzato con altri mezzi
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: assenza di cifratura e separazione dei dati sensibili da quelli personali con violazione misure minime ABSC 13 (CSC 13): PROTEZIONE DEI DATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta

copia informatica per consultazione

Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- L'assenza di modalita' organizzative e interventi formativi per la corretta gestione degli identificativi e delle password non osta a che l'obiettivo di una corretta gestione venga raggiunto con altri mezzi
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: assenza di profili d'accesso differenziati e utilizzo delle utenze amministrative senza privilegi con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: assenza di protezione contro il rischio di intrusione con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: esposizione di password in chiaro e/o gestione non corretta delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: mancanza di automatismi per l'aggiornamento delle password con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Medio bassa	- La mancanza di automatismi per l'aggiornamento delle password non equivale, in automatico, a violazione dei dati
Ufficio gestione giuridica del personale dipendente	- OPERATORI: elenco degli incaricati accessibile	Medio bassa	- L'elenco degli incaricati accessibile non equivale, in automatico, a lesione dei dati
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: mancanza, inadeguatezza o inutilizzazione delle procedure di backup, con omessa effettuazione delle copia di sicurezza con violazione misure minime ABSC 10 (CSC 10): COPIE DI SICUREZZA (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: presenza di codice non conforme alle specifiche del programma con violazione misure minime ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: replicabilita' delle parole chiave con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: sistema di autenticazione assente o non adeguato con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: sottrazione strumenti contenenti dati	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: sottrazione documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: ingressi non autorizzati ad aree e locali	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: malfunzionamento sistemi di climatizzazione	Alta	- Il malfunzionamento sistemi di climatizzazione non equivale, in automatico, a fattore incidente su lesione di dati
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: uso non autorizzato di hardware o di software e, in particolare, installazione ed esecuzione di software non autorizzato e non gestito con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI e ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: manomissione o sabotaggio sistemi con violazione misure minime ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: errori di configurazione di hardware e software e/o assenza di configurazioni sicure standard per la protezione dei sistemi operativi con violazione misure minime ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- OPERATORI: accesso non autorizzato ai documenti cartacei	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- OPERATORI: assenza di consapevolezza, incuria, trascuratezza, disattenzione	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: assenza di controlli e monitoraggi sul funzionamento del sistema di sicurezza	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: assenza di integrazione delle misure di sicurezza nei processi/procedimenti	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: assenza di istruzioni operative	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: assenza di inserimento degli illeciti in materia di trattamento dati nel PTPC	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- OPERATORI: errore nell'utilizzo della posta elettronica con invio di e-mail ad un destinatario sbagliato	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- CONTESTO: divulgazione dati allo sportello (front-office) per mancanza di chiusura e presenza di persone in coda	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: utilizzo di parole chiavi non adeguate con violazione misure minime ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Altissima	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' molto alta
Ufficio gestione giuridica del personale dipendente	- APPARECCHIATURE-ICT: assenza di log da cui risalire ai tentativi di accesso o di manomissione con violazione misure minime ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni)	Alta	- Visto dalla prospettiva degli interessati, questa tipologia di rischio non puo' che avere una gravita' alta

copia informatica per consultazione

SERVIZIO	Indice trattamento	Misure informatiche
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 09 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure
Attivita' Trasversali	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Consiglio comunale e commissioni consiliari	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Consiglio comunale e commissioni consiliari	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Consiglio comunale e commissioni consiliari	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Gestione Patrimonio Immobiliare	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

copia informatica per consultazione

Gestione Patrimonio Immobiliare	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Gestione Patrimonio Immobiliare	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Giunta comunale	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Giunta comunale	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

copia informatica per consultazione

Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Giunta comunale	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Giunta comunale	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Segretario Comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Segretario Comunale	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Segretario Comunale	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Segretario Comunale	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizi Finanziari	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	inventariando e mantenendo aggiornato l'inventario, in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

Servizi Legali	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizi Legali	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Ambiente e Infrastrutture	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Ambiente e Infrastrutture	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

copia informatica per consultazione

Servizio Ambiente e Infrastrutture	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Ambiente e Infrastrutture	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Ambiente e Infrastrutture	Scheda n. 52 - Ufficio Ambiente - Trattamento di dati relativi all'attivita' di gestione dei rifiuti	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Attivita' Economiche	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Bilancio	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	inventariati nodi e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure
Servizio Demanio	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio di Protezione Civile	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Economato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure
Servizio Economato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

copia informatica per consultazione

Servizio Lavori Pubblici	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Lavori Pubblici	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Notifica	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Polizia Ammistrativa	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Polizia Ammistrativa	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Polizia Ammistrativa	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Polizia Urbana	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Polizia Urbana	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Polizia Urbana	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Scuola e Biblioteca	Scheda n. 11 - Servizi sociali - Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Scuola e Biblioteca	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Scuola e Biblioteca	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Scuola e Biblioteca	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Scuola e Biblioteca	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	inventariato ed mantenuto aggiornato l'inventario in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure
Servizio Scuola e Biblioteca	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria e Protocollo	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Segreteria e Protocollo	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria e Protocollo	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	inventariando e mantenendo aggiornato l'inventario, in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 15 - Servizi sociali - Trattamento di dati relativi all'attivita' di gestione dell'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 55 - Servizi Sociali - Trattamento di dati relativi all'attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al "Sistema di protezione dei richiedenti asilo e rifugiati"	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Tributi	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,

copia informatica per consultazione

Servizio Tributi	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,
Servizio Urbanistica	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Servizio Urbanistica	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Sindaco	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)

copia informatica per consultazione

Ufficio Gestione economica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software autorizzati in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software autorizzati in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Ufficio gestione giuridica del personale dipendente	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, inventariando e mantenendo aggiornato l'inventario, in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)
Ufficio gestione giuridica del personale dipendente	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure

copia informatica per consultazione

SERVIZIO	Indice trattamento	Misure logistiche
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 09 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Attivita' Trasversali	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Consiglio comunale e commissioni consiliari	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Consiglio comunale e commissioni consiliari	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Consiglio comunale e commissioni consiliari	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Gestione Patrimonio Immobiliare	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Gestione Patrimonio Immobiliare	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Gestione Patrimonio Immobiliare	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Giunta comunale	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Giunta comunale	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Giunta comunale	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Giunta comunale	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Segretario Comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Segretario Comunale	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Segretario Comunale	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Segretario Comunale	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizi Finanziari	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizi Legali	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizi Legali	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Ambiente e Infrastrutture	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Ambiente e Infrastrutture	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Ambiente e Infrastrutture	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Ambiente e Infrastrutture	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Ambiente e Infrastrutture	Scheda n. 52 - Ufficio Ambiente - Trattamento di dati relativi all'attivita' di gestione dei rifiuti	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Attivita' Economiche	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Bilancio	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Demanio	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio di Protezione Civile	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Economato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Economato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Lavori Pubblici	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Lavori Pubblici	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Notifica	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Polizia Ammistrativa	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Polizia Ammistrativa	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Polizia Ammistrativa	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Polizia Urbana	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Polizia Urbana	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Polizia Urbana	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Scuola e Biblioteca	Scheda n. 11 - Servizi sociali - Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Scuola e Biblioteca	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Scuola e Biblioteca	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Scuola e Biblioteca	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Scuola e Biblioteca	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Scuola e Biblioteca	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria e Protocollo	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria e Protocollo	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Segreteria e Protocollo	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 15 - Servizi sociali - Trattamento di dati relativi all'attivita' di gestione dell'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 55 - Servizi Sociali - Trattamento di dati relativi all'attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al "Sistema di protezione dei richiedenti asilo e rifugiati"	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Tributi	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Tributi	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Servizio Urbanistica	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Servizio Urbanistica	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Sindaco	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Ufficio Gestione economica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Ufficio gestione giuridica del personale dipendente	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere
Ufficio gestione giuridica del personale dipendente	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere

copia informatica per consultazione

SERVIZIO	Indice trattamento	Misure organizzative
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 09 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Attivita' Trasversali	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Consiglio comunale e commissioni consiliari	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Consiglio comunale e commissioni consiliari	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Gestione Patrimonio Immobiliare	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Gestione Patrimonio Immobiliare	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Gestione Patrimonio Immobiliare	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Giunta comunale	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Giunta comunale	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Giunta comunale	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Giunta comunale	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Segretario Comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Segretario Comunale	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Segretario Comunale	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Segretario Comunale	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Servizi Finanziari	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizi Legali	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizi Legali	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Ambiente e Infrastrutture	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Servizio Ambiente e Infrastrutture	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Ambiente e Infrastrutture	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Ambiente e Infrastrutture	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Ambiente e Infrastrutture	Scheda n. 52 - Ufficio Ambiente - Trattamento di dati relativi all'attivita' di gestione dei rifiuti	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Servizio Attivita' Economiche	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Bilancio	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Demanio	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Servizio di Protezione Civile	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli
Servizio Economato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Economato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Lavori Pubblici	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Lavori Pubblici	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Notifica	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Polizia Ammistrativa	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli
Servizio Polizia Ammistrativa	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli
Servizio Polizia Ammistrativa	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli
Servizio Polizia Urbana	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli

copia informatica per consultazione

Servizio Polizia Urbana	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Polizia Urbana	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Scuola e Biblioteca	Scheda n. 11 - Servizi sociali - Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Scuola e Biblioteca	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Scuola e Biblioteca	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Scuola e Biblioteca	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Scuola e Biblioteca	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Scuola e Biblioteca	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Segreteria e Protocollo	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria e Protocollo	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria e Protocollo	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 15 - Servizi sociali - Trattamento di dati relativi all'attivita' di gestione dell'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 55 - Servizi Sociali - Trattamento di dati relativi all'attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al "Sistema di protezione dei richiedenti asilo e rifugiati"	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Servizio Tributi	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Tributi	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Urbanistica	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Servizio Urbanistica	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Sindaco	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale
Ufficio Gestione economica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale

copia informatica per consultazione

Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Ufficio gestione giuridica del personale dipendente	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici
Ufficio gestione giuridica del personale dipendente	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici

copia informatica per consultazione

SERVIZIO	Indice trattamento	Misure procedurali
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 09 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - PROCEDURA OPERATIVA (PO): definire e attuare procedura operativa per dare attuazione, nell'attivita' di videosorveglianza, al principio di c.d. proporzionalita' nella scelta delle modalita' di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonche' nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalita' perseguite - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Attivita' Trasversali	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Consiglio comunale e commissioni consiliari	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Consiglio comunale e commissioni consiliari	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Consiglio comunale e commissioni consiliari	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Gestione Patrimonio Immobiliare	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Gestione Patrimonio Immobiliare	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Gestione Patrimonio Immobiliare	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Giunta comunale	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Giunta comunale	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Giunta comunale	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Giunta comunale	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Segretario Comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Segretario Comunale	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Segretario Comunale	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Segretario Comunale	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizi Finanziari	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizi Legali	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizi Legali	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Ambiente e Infrastrutture	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Ambiente e Infrastrutture	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Ambiente e Infrastrutture	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Ambiente e Infrastrutture	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Ambiente e Infrastrutture	Scheda n. 52 - Ufficio Ambiente - Trattamento di dati relativi all'attivita' di gestione dei rifiuti	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Attivita' Economiche	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Bilancio	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Demanio	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio di Protezione Civile	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Economato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Economato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Lavori Pubblici	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Lavori Pubblici	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Notifica	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Ammistrativa	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Ammistrativa	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Ammistrativa	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Polizia Urbana	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Urbana	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Urbana	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 11 - Servizi sociali - Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Scuola e Biblioteca	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Scuola e Biblioteca	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria e Protocollo	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria e Protocollo	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria e Protocollo	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 15 - Servizi sociali - Trattamento di dati relativi all'attivita' di gestione dell'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 55 - Servizi Sociali - Trattamento di dati relativi all'attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al "Sistema di protezione dei richiedenti asilo e rifugiati"	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Tributi	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Tributi	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Urbanistica	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Urbanistica	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Sindaco	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Ufficio Gestione economica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Ufficio gestione giuridica del personale dipendente	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Ufficio gestione giuridica del personale dipendente	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

SERVIZIO	Indice trattamento	Misure logistiche	Misure informatiche	Misure organizzative	Misure procedurali
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 03 - Servizi demografici/Anagrafe - Trattamento di dati relativi alla gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 04 - Servizi demografici/Stato civile - Trattamento di dati relativi all'attivita' di gestione dei registri di stato civile	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 05 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' relativa all'elettorato attivo e passivo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 06 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta degli albi degli scrutatori e dei presidenti di seggio	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 07 - Servizi demografici/Elettorale - Trattamento di dati relativi all'attivita' di tenuta dell'elenco dei giudici popolari	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 09 - Servizi demografici/Leva - Trattamento di dati relativi all'attivita' di tenuta delle liste di leva e dei registri matricolari	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 41 - Ufficio Comunale di statistica - Trattamento di dati per scopi statistici effettuati da SISTAN (Ufficio Comunale di statistica)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - PROCEDURA OPERATIVA (PO): definire e attuare procedura operativa per dare attuazione, nell'attivita' di videosorveglianza, al principio di c.d. proporzionalita' nella scelta delle modalita' di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonche' nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalita' perseguite - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Anagrafe, Stato Civile, Elettorale, Leva, Statistica e Polizia Mortuaria	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Attivita' Trasversali	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Consiglio comunale e commissioni consiliari	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Consiglio comunale e commissioni consiliari	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Consiglio comunale e commissioni consiliari	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Consiglio comunale e commissioni consiliari	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Gestione Patrimonio Immobiliare	Scheda n. 20 - Trattamenti relativi alla attivita' di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Gestione Patrimonio Immobiliare	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Gestione Patrimonio Immobiliare	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Gestione Patrimonio Immobiliare	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Gestione Patrimonio Immobiliare	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Giunta comunale	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Giunta comunale	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Giunta comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Giunta comunale	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Giunta comunale	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Segretario Comunale	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Segretario Comunale	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Segretario Comunale	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Segretario Comunale	Scheda n. 60 - Ufficio Segreteria/Contratti - Trattamento di dati relativi all'attivita' contrattuale (controlli, stipula, diritti di segreteria/rogito, repertorio)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Segretario Comunale	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizi Finanziari	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizi Legali	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizi Legali	Scheda n. 30 - Avvocatura - Trattamento di dati relativi all'attivita' di consulenza giuridica, nonche' al patrocinio ed alla difesa in giudizio dell'amministrazione nonche' alla consulenza e copertura assicurativa in caso di responsabilita' civile verso terzi dell'amministrazione	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Ambiente e Infrastrutture	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Ambiente e Infrastrutture	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Ambiente e Infrastrutture	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Ambiente e Infrastrutture	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Ambiente e Infrastrutture	Scheda n. 52 - Ufficio Ambiente - Trattamento di dati relativi all'attivita' di gestione dei rifiuti	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Attivita' Economiche	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Bilancio	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Bilancio	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Demanio	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio di Protezione Civile	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando ad tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, inventariandoli e mantenendo aggiornato l'inventario) in modo che	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Economato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando ad tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Economato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando ad tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Edilizia	Scheda n. 46 - Ufficio Edilizia Privata - Trattamento di dati relativi ai titoli abilitativi edilizi, esclusi i titoli concernenti l'abbattimento di barriere architettoniche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Lavori Pubblici	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Lavori Pubblici	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Lavori Pubblici	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Notifica	Scheda n. 57 - Ufficio Segreteria/Notifiche - Trattamento di dati relativi all' attivita' di tenuta dell'albo e delle notifiche dell'Ente	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Polizia Ammistrativa	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Ammistrativa	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Ammistrativa	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Urbana	Scheda n. 25 - Polizia municipale - Trattamento di dati relativi alla gestione delle procedure sanzionatorie	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Polizia Urbana	Scheda n. 26 - Polizia municipale - Trattamento di dati relativo all'attivita' di polizia annonaria, commerciale ed amministrativa	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi manionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Polizia Urbana	Scheda n. 27 - Polizia municipale - Trattamento di dati relativi all'attivita' di vigilanza edilizia, in materia di ambiente e sanita', nonche' di polizia mortuaria	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi manionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 11 - Servizi sociali - Trattamento di dati relativi all'attivita' di assistenza scolastica ai portatori di handicap o con disagio psico-sociale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-01- PROCEDURA OPERATIVA (PO): definizione e attuazione procedure operative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati in relazione alle finalita' - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Scuola e Biblioteca	Scheda n. 21 - Istruzione e cultura - Trattamento di dati relativi alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Scuola e Biblioteca	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria e Protocollo	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria e Protocollo	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria e Protocollo	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 31 - Politiche del lavoro - Trattamento di dati relativi all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 32 - Trattamento di dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonche' dei rappresentanti dell'ente presso enti, aziende e istituzioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 33 - Trattamento di dati relativi all'attivita' politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attivita' istituzionale degli organi comunali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 47 - Ufficio Segreteria - Trattamento di dati relativi alla definizione delle modalita' di gestione dei servizi pubblici (convenzioni, concessioni, in house, etc.)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 48 - Ufficio Segreteria/RPCT - Trattamento di dati relativi alla gestione del rischio di corruzione e di illegalita'	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 49 - Uffici Segreteria e Ragioneria - Trattamento di dati relativi a transazioni, lasciti, donazioni o altri atti di straordinaria amministrazione ovvero accordi integrativi o sostitutivi del provvedimento	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 51 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione dell'accesso a documenti amministrativi, dell'accesso civico semplice e generalizzato	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 58 - Ufficio per le relazioni con il pubblico-U.R.P. - Trattamento dati relativi alle relazioni con il pubblico (ricevimenti, telefonate, mail, etc.)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 59 - Ufficio C.E.D. - Trattamento di dati relativi all'attivita' di gestione hardware, software, server, personal computer clients, rete	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 61 - Ufficio Segreteria/Protocollo e Archivio - Trattamento di dati relativi all'attivita' di protocollazione e archiviazione	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Segreteria Sindaco e Relazioni Esterne	Scheda n. 62 - Ufficio Ragioneria/Programmazione e Pianificazione - Trattamento di dati relativi all'attivita' di gestione economica, finanziaria, programmazione e provveditorato inclusa la relativa movimentazione finanziaria, la gestione delle fatture, inventario e cassa economale	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 10 - Servizi sociali - Trattamento di dati relativi alla attivita' di assistenza domiciliare	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 12 - Servizi sociali - Trattamento di dati relativi alla attivita' di gestione delle richieste di ricovero o inserimento in istituti, Case di cura, Case di riposo, ecc	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 14 - Servizi sociali - Trattamento di dati relativi alla attivita' di valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 15 - Servizi sociali - Trattamento di dati relativi all'attivita' di gestione dell'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 16 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 18 - Servizi sociali - Trattamento di dati relativi all'attivita' di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, [illegible]	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 22 - Istruzione e cultura - Trattamento di dati relativi relativi all'attivita' di formazione ed in favore del diritto allo studio	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 37 - Ufficio Segreteria e tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi all'attivita' di conferimento di onorificenze e ricompense nonche' concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 39 - Uffici Cultura, Sport, Manifestazioni - Trattamento di dati relativi alle attivita' ricreative, di promozione della cultura e dello sport ed occupazioni di suolo pubblico	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 44 - Ufficio Patrimonio - Trattamento di dati relativi all'attivita' di gestione beni demaniali e patrimoniali, incluse le manutenzioni, la gestione di locazioni e di contratti di partenariato pubblico-privato (es.interventi di sussidiarieta')	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Socio Culturale, Sport e Volontariato	Scheda n. 50 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di programmazione, progettazione, affidamento, di aggiudicazione e di esecuzione di contratti pubblici, inclusi i contratti di partenariato pubblico-privato e le convenzioni con il terzo settore e incluse le liquidazioni di acconti o saldi	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 55 - Servizi Sociali - Trattamento di dati relativi all'attivita' di gestione dell'accoglienza dei richiedenti asilo e rifugiati da parte degli enti locali partecipanti al "Sistema di protezione dei richiedenti asilo e rifugiati"	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Socio Culturale, Sport e Volontariato	Scheda n. 56 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di gestione del sito web dell'Ente, incluse le pubblicazioni obbligatorie in attuazione degli obblighi di trasparenza	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Tributi	Scheda n. 38 - Ufficio Tributi - Trattamento di dati relativi alle agevolazioni tributarie e alla gestione dei tributi locali	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Servizio Tributi	Scheda n. 42 - Tutti gli uffici/Attivita' trasversale - Trattamento di dati relativi all'attivita' di controllo, di ispezione, comprese le attivita' di validazione dei progetti e di sopralluogo	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Tributi	Scheda n. 43 - Ufficio Ragioneria - Trattamenti relativi all'attivita' di liquidazione e di pagamento di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Urbanistica	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Servizio Urbanistica	Scheda n. 64 - Tutti gli uffici - Attivita' trasversale - Trattamento di dati relativi al rilascio di autorizzazioni diverse dalla autorizzazioni per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza, e trattamenti di dati per verifiche e controlli e certificazioni	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-09 - ESERCIZIO DIRITTI: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-15 - SISTEMA GESTIONE PRIVACY: prescrizione di linee - guida di sicurezza - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-05 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per la gestione delle credenziali di autenticazione - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Sindaco	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Sindaco	Scheda n. 36 - Ufficio tecnico - Trattamento di dati relativi all'attivita' di protezione civile, incluse la prevenzione e l'eliminazione di gravi pericoli che minacciano l'incolumita' pubblica e la sicurezza urbana inclusi i censimenti dei danni e le ordinanze contingibili e urgenti	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Sindaco	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	- ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare)	- MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Ufficio Gestione economica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato,	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-17 - GESTIONE DATI: altre istruzioni interne - MS-ORG-19 - SISTEMA GESTIONE PRIVACY: redazione di appositi mansionari - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

Ufficio gestione giuridica del personale dipendente	Scheda n. 01 - Personale/Trattamento di dati relativi all'attivita' di gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Ufficio gestione giuridica del personale dipendente	Scheda n. 02 - Personale/Trattamento di dati relativi alla gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attivita' relativa al riconoscimento di benefici connessi all'invalidita' civile per il personale e all'invalidita' derivante da cause di servizio, nonche' da riconoscimento di inabilita' a svolgere attivita' lavorativa	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	(Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 13 (CSC 13) - Protezione dati: processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrita' delle informazioni rilevanti (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-10 - INFORMAZIONE: informazione continua e aggiornamento costante su procedure operative e istruzioni - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-07 - GESTIONE DATI: distruzione documenti non necessari - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-02 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante - MS-PO-07 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia: a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; b) le misure di ripristino in caso di data breach - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.
Ufficio gestione giuridica del personale dipendente	Scheda n. 45 - Segreteria e tutti gli Uffici- Attivita' trasversale - Trattamento di dati relativi all'attivita' di regolamentazione, programmazione, pianificazione (Statuti, Regolamenti, Programmi, Piani, Criteri generali, Direttive, Indirizzi, e altri atti amministrativi generali) e progettazione, inclusi i trattamenti per riunioni, tavoli, consulte	- MS-LOG-10 - PROTEZIONE AREE E LOCALI: continuita' dell'alimentazione elettrica - MS-LOG-12 - PROTEZIONE AREE E LOCALI: deposito in cassaforte - MS-LOG-13 - PROTEZIONE AREE E LOCALI: custodia in classificatori o armadi non accessibili MS-LOG-100 - PROTEZIONE AREE E LOCALI: sicurezza antifurto con applicazione di serrature in tutte le porte degli uffici MS-LOG-200 - PROTEZIONE AREE E LOCALI: sistema antincendio della sede principale e delle sedi secondarie con applicazione di estintori/impianto antincendio, impianti di climatizzazione e implementazione dei controlli di adeguatezza e regolarita' impianti MS-LOG-800 - PROTEZIONE AREE E LOCALI: autorizzazione scritta e previsione di specifici impegni comportamentali nel capitolato d'appalto e relativa fornitura ai dipendenti dell'impresa di pulizie di apposito permesso di accesso agli uffici fuori dall'orario di lavoro, con dettagliate istruzioni circa il comportamento da tenere	Inventariando e mantenendo aggiornato l'inventario in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 04 (CSC 4) - valutazione e correzione continua della vulnerabilita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 05 (CSC 5) - uso appropriato dei privilegi di amministratore: regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 08 (CSC 8) - difese contro i malware: controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dall'Ente e relative implementazioni effettuate dal titolare) - ABSC 10 (CSC 10) - copie di sicurezza: procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, cosi' da consentirne il ripristino in caso di necessita' (Elenco ufficiale Agid delle 'Misure minime per la sicurezza ICT delle pubbliche amministrazioni' e relative implementazioni effettuate dal titolare) - ABSC 02 (CSC 2) - inventario dei software autorizzati e non autorizzati: gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione (Elenco ufficiale Agid delle 'Misure	- MS-ORG-04 - TRATTAMENTI SENZA L'USO DI STRUMENTI ELETTRONICI: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative - MS-ORG-03 - FORMAZIONE: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri - MS-ORG-06 - GESTIONE DATI: separazione documenti e dati in relazione alla natura dei dati medesimi e al contesto di riferimento - MS-ORG-08 - GESTIONE DATI: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonche' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del Garante - MS-ORG-05 - GESTIONE DATI: adeguate modalita' di utilizzazione dei documenti - MS-ORG-13 - CULTURA DELLA PREVENZIONE: dotazione di un apposito software per la gestione del rischio e la valutazione di impatto - MS-ORG-14 - CULTURA DELLA PREVENZIONE: dotazione di specifici supporti conoscitivi e informativi costituiti, tra cui la Banca dati privacy, nonche' di un servizio specialistico di consulenza accessibile da tutti gli incaricati e da tutti i dipendenti - MS-ORG-16 - SISTEMA GESTIONE PRIVACY: analisi dei rischi - MS-ORG-18 - SISTEMA GESTIONE PRIVACY: assegnazione di incarichi - MS-ORG-20 - SISTEMA GESTIONE PRIVACY: formazione professionale - MS-ORG-21 - SISTEMA GESTIONE PRIVACY: documentazione dei controlli periodici	- MS-PO-09 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi - MS-PO-10 - PROCEDURA OPERATIVA (PO): definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali; b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del RGDP.

copia informatica per consultazione

COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione n. 39 del 07/03/2025

Assessore Proponente: MONTAUTI DAVIDE

OGGETTO: APPROVAZIONE DOCUMENTO AGGIORNATO "MISURE MINIME DI SICUREZZA ICT" DI CUI ALLA CIRCOLARE AGID N. 2/2017

L'anno duemilaventicinque addì sette del mese di marzo alle ore 12:00 nella Casa Comunale, previa l'osservanza di tutte le formalità prescritte dalla vigente Legge Comunale e Provinciale, sono stati convocati oggi a seduta i componenti della Giunta Comunale, che nelle persone seguenti risultano presenti alla trattazione della proposta di deliberazione in oggetto:

MONTAUTI DAVIDE	SINDACO	Presente
PAOLINI CHIARA	VICE SINDACO	Presente (Skype)
MAI DANIELE	ASSESSORE	Assente
LENZI STEFANO	ASSESSORE	Presente (Skype)
SPINETTI JACOPO	ASSESSORE	Assente

Presenti n. 3 Assenti n. 2

Partecipa il SEGRETARIO ROSSI ANTONELLA che provvede alla redazione del presente verbale.
Presiede la seduta, nella sua qualità di SINDACO, il Sig. MONTAUTI DAVIDE che dichiara aperta la trattazione dell'oggetto sopra indicato.

copia informatica per consultazione

Deliberazione n. 39 del 07/03/2025

LA GIUNTA COMUNALE

Premesso che:

- gli attacchi informatici ai sistemi rappresentano oggi un elemento di grande criticità per le pubbliche amministrazioni e le aziende private;
- l'attenzione del legislatore e del governo nazionale ed europeo è volta ad attività di prevenzione e difesa rispetto agli attacchi informatici e più in generale a favorire le azioni di ICT Security delle Pubbliche Amministrazioni;
- in questo contesto sono stati emanati vari provvedimenti legislativi, tra cui la Legge lì. 133/2019 sul perimetro cibernetico, che vuole contribuire ad innalzare la sicurezza del sistema Paese verso le minacce cyber, individuando, da un lato, alcuni obblighi in capo a coloro che gestiscono infrastrutture essenziali per il Paese e, dall'altro, definendo un'architettura in grado di valutare ex-ante l'adeguatezza dei diversi componenti informatici che andranno ad essere utilizzati da tali gestori e s.m.i. (vedi anche DPCM del 24 Gennaio 2013 recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", il DPCM 27 gennaio 2014 che approva il "quadro strategico nazionale per la sicurezza dello spazio cibernetico" e la direttiva 1 agosto 2015 della Presidenza del Consiglio "Sistema di informazione per la sicurezza della Repubblica");

Visti:

- l'art.14 bis del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera a), tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D. anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica;
- la direttiva dell'agosto 2015 del Presidente del Consiglio dei Ministri che ha imposto l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici e che al fine di agevolare tale processo, ha individuato nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento;
- la Circolare di AgID del 18 aprile 2017, n. 2/2017 denominata "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni" che ha introdotto l'insieme dei controlli che costituiscono le Misure Minime AgID, denominati AgID Basic Security Controls (ABSC);

Considerato che:

- la citata circolare prevede che ciascuna Amministrazione debba non solo implementare i controlli rilevanti, ma anche dare brevemente conto della modalità di implementazione compilando un apposito modulo, da conservare secondo le modalità stabilite dall'Amministrazione stessa e da inviarlo al CERT-PA in caso di incidenti;
- il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation Regolamento UE 2016/679) - intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea aumentando il livello di respon-

copia informatica per consultazione

sabilizzazione ed introducendo il concetto di misure idonee alle organizzazioni che sono chiamate ad attuare quanto necessario per la sicurezza informatica dei dati;

Dato atto che:

- al fine di non costringere le Amministrazioni, soprattutto quelle più piccole, ad introdurre misure eccessive per la propria organizzazione, con evidente dispendio di risorse, i singoli controlli CSC sono stati trasposti nei controlli ABSC suddividendoli in famiglie di misure di dettaglio più fine, che possono essere adottate in modo indipendente proprio per consentire alle Amministrazioni di graduare il proprio sistema di sicurezza per meglio adattarlo alle effettive esigenze della specifica realtà locale;
- per facilitare ulteriormente l'adozione, minimizzando gli impatti implementativi sull'organizzazione interessata, i controlli sono inoltre stati suddivisi in tre gruppi, riferiti a livelli complessivi di sicurezza crescente, che differenziano quelli strettamente necessari da quelli via via più critici rispetto alle informazioni trattate ed ai servizi erogati;
- il Comune di Campo nell'Elba aveva già provveduto a far redigere il documento di che trattasi, conservato agli atti di questi uffici dalla data del 27.12.2017;

Dato atto, altresì, che dal 2017 ad oggi il sistema informativo dell'Ente ha subito modifiche sia relative ai programmi utilizzati che all'architettura fisica, e pertanto è stata richiesta una attività di revisione e aggiornamento del documento contenente le misure minime di sicurezza all'operatore economico titolare della manutenzione HW e SW, ADS spa;

Rilevato che lo stesso ha provveduto a trasmettere il documento di cui al paragrafo precedente, opportunamente revisionato ed aggiornato, con nota protocollo N. 3359 del 05.03.2025;

Visto pertanto l'allegato modulo di implementazione di cui all'allegato 2 della circolare N.2 del 18 aprile 2017, n.2/2017 emanata dalla Agenzia per l'Italia Digitale, debitamente aggiornato ed allegato al presente atto a farne parte integrante e sostanziale, e ritenuto di doverlo approvare, anche al fine della sua integrazione all'interno di altra documentazione inerente la sicurezza dei dati, quale ad esempio non esaustivo il piano di protezione dei dati personali e di gestione del rischio di violazione di cui alla normativa inerente il GDPR;

Acquisito il parere favorevole espresso in ordine alla regolarità tecnica, ai sensi dell'art. 49 comma 1, del D.LGS. 267/2000, da parte del Responsabile del Servizio interessato;

Rilevato che il presente atto non necessita dell'acquisizione del parere di regolarità contabile ex art. 49 del D.LGS. 267/2000 in quanto non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente;

All'unanimità dei voti espressi nelle forme di legge

D E L I B E R A

1. di approvare i richiami, le premesse e l'intera narrativa quali parti integranti e sostanziali del presente atto;

2. di approvare altresì il modulo, opportunamente revisionato ed aggiornato al mese di febbraio 2025, di implementazione delle misure minime di sicurezza ICT per le

copia informatica per consultazione

pubbliche amministrazioni, allegato al presente atto a farne parte integrante e sostanziale, in attuazione della circolare AgID nº 2/2017;

3. di dichiarare il presente atto immediatamente eseguibile, ai sensi dell'art. 134 del D.Lgs. n.267/2000, in considerazione della necessità di rendere disponibile quanto prima la versione aggiornata del documento al fine della sua eventuale integrazione all'interno di altra documentazione inerente la sicurezza dei dati;

copia informatica per consultazione

COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

Verbale n. 9 del 07.03.2025

IL SINDACO
MONTAUTI DAVIDE

IL SEGRETARIO
ROSSI ANTONELLA

copia informatica per consultazione

MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA PER LE PUBBLICHE AMMINISTRAZIONI
ULTIMO AGGIORNAMENTO – FEBBRAIO 2025

Il presente modello fornisce un ausilio per determinare il livello di copertura prodotto dalle misure poste in essere dall'amministrazione attraverso l'indicazione, nella colonna "Modalità di implementazione", dello strumento effettivamente utilizzato per realizzare lo ABSC riferito alla riga.

Per misura si intende non solo lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Pertanto, al fine di fornire tutte le principali informazioni identificative e descrittive relative alle singole misure può essere utile fare riferimento anche alle informazioni contenute in procedure, eventualmente, già approvate e adottate dall'Amministrazione che si raccomanda di fornire in allegato in caso di segna- lazione di incidente informatico al CERT-PA

Le indicazioni delle modalità di implementazione possono essere ulteriormente utili anche come punto di riferimento dello stato della sicurezza dei servizi/si- stemi dell'Amministrazione.

Il modulo deve essere compilato e firmato digitalmente con marcatura temporale dal Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, dal dirigente allo scopo designato e dal Responsabile Legale della struttura.

Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	Modalità di Implementazione	L
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Implementato: oltre all'inventario fisico/contabile dell'HW, viene gestito un inventario per singola macchina attiva da parte della società titolare della manutenzione HW e SW. Regolarmente aggiornato.	M
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Viene effettuato in maniera semi automatica via server	S
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalia	Non implementato	A
		4	Qualificare i sistemi connessi alla rete **a**ttraverso l'analisi del loro traffico.	Implementato: gestione della società titolare della manutenzione HW e SW	A
	2	1	Implementare il "logging" delle operazione del server DHCP.	Implementato: gestione della società titolare della manutenzione HW e SW.	S
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Implementato: gestione della società titolare della manutenzione HW e SW	S
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Non implementato.	S

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	Implementato: viene indentificato l'IP macchina/nome macchina e utente. Il titolare/responsabile ufficio viene identificato dalla macro e microstruttura amministrativa dell'ente. Di pari passo è possibile identificare se il dispositivo è portatile/personale.	S
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	Implementato: correlato con il punto 1.4.2 Per i cellulari che si collegano alla rete sono identificati con IP e nome dispositivo. Per i cellulari non collegati nessuna identificazione	A
	5	1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	Implementato: tutti i dispositivi per accedere alla rete locali devono sottostare a procedure di autenticazione. Tutti i dispositivi connessi via cavo sono autorizzati ad andare in internet, cosi come i dispositivi wifi previa password. Un firewall si occupa degli accessi e dei log.	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Non implementato l’accesso mediante certificati digitali. Tuttavia, nessuno può collegarsi da remoto alla rete locale in quanto protetta da firewall con accessi limitati.	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC_ID #			Descrizione	Modalità di Implementazione
2	1	1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, work-station e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.	Implementato: esiste un elenco del software autorizzato. Teoricamente ogni utente è amministratore della propria postazione ed è a conoscenza che l'installazione di altro software non è consentita se non previo accordo con il soggetto responsabile della rete. In ogni caso, eventuali danni all'infrastruttura è diretta responsabilità dell'utente.
	2	1	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	Implementato su server: gestione della società titolare della manutenzione HW e SW Non implementato su configurazioni locali
		2	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	Implementato su server: gestione della società titolare della manutenzione HW e SW. Non implementato su configurazioni locali
		3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Non implementato.

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
2	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Implementato: gestione della società titolare della manutenzione HW e SW. Regolarmente (tempistiche stabilite dalla stessa società) viene eseguita regolare scansione antivirus e malware.	M
		2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Implementato: gestione della società titolare della manutenzione HW e SW.	S
		3	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	Eseguito in maniera non automatica ma da parte di operatore.	A
	4	1	Utilizzare macchine virtuali e/o sistemi air-gapped[1] per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	Reverse Proxy situato in una rete DMZ isolata dalla rete del comune, per gestire gli accessi ai vari portali messi a disposizione dall'ente.	A

1 Air-gapped: isolato. Tecnica informatica solitamente utilizzata per mettere in sicurezza sistemi o reti che richiedono maggior attenzione rispetto ad altre: basti pensare alle reti classificate come militari, ai sistemi di controllo di grande aziende e industrie sensibili (ad esempio centrali nucleari o industrie chimiche) o *network* che gestiscono e processano pagamenti attraverso carte di credito e bancomat.

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	Implementato: gestione della società titolare della manutenzione HW e SW. Limitatamente ai server.	S
		3	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	Implementato: gestione della società titolare della manutenzione HW e SW. Limitatamente ai server.	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
3	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Implementato: gestione della società titolare della manutenzione HW e SW.	M
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Implementato: gestione della società titolare della manutenzione HW e SW.	M
		3	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Non implementato.	S
	3	1	Le immagini d'installazione devono essere memorizzate offline.	Implementato in passato. Eventualmente da implementare dopo futura valutazione	M
		2	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti	Non implementato. In esito alla valutazione di cui al punto 3.3.1, in caso di valutazione positiva, verrà implementato.	S
	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Implementato: gestione della società titolare della manutenzione HW e SW. Connessioni protette via VPN.	M

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	5	1	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Non implementato	S
		2	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	Non implementato	A
		3	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	Implementato: gestione della società titolare della manutenzione HW e SW solo su apparati HW Server	A
		4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Implementato: gestione della società titolare della manutenzione HW e SW solo su apparati HW Server	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

	6	1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Non implementato	A
	7	1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Non implementato	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
4	1	1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Non implementato. Tuttavia va considerato che l'accesso è protetto da firewall con accessi molto limitati.	M
		2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Non implementata con carattere periodico. In caso di notizie di potenziali minacce si procede ad analisi sulla base dei bollettini di sicurezza internet.	S
		3	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	Non implementato.	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Non implementato	S
		2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Non implementato	S
		3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile	Non implementato	S
	3	1	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	Implementato: gestione della società titolare della manutenzione HW e SW nel caso di controllo antivirus	S
		2	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	Implementato: gestione della società titolare della manutenzione HW e SW nel caso di controllo antivirus	S

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Implementato: antivirus e antimalware vengono periodicamente aggiornati	M
		2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione.	Implementato: gestione della società titolare della manutenzione HW e SW (aggiornamento con servizi di bollettini sulla sicurezza informatica)	S
ABSC_ID #			**Descrizione**	**Modalità di Implementazione**	**Liv**
	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applica-zioni.	Implementato: gestione della società titolare della manutenzione HW e SW sui server. Sulle singole postazioni l'onere è sul singolo operatore. I SW applicativi vengono aggiornati dalle rispettive case madri.	M
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non esiste la fattispecie	M
	6	1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Implementato: gestione della società titolare della manutenzione HW e SW	S

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

	7	1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	Non implementato	S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
		1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Implementato: gestione della società titolare della manutenzione HW e SW	M

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

4		2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più prioritarie	Implementato: gestione della società titolare della manutenzione HW e SW	M
	9	1	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	Non implementato	S
	10	1	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Non implementato	S

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
5	1	1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Implementato: gestione della società titolare della manutenzione HW e SW limitatamente ai server	M
		2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Implementato: gestione della società titolare della manutenzione HW e SW limitatamente ai server	M
		3	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Implementato: gestione della società titolare della manutenzione HW e SW	S
		4	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Non implementato	A
	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Non implementato	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
5	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Implementato: gestione della società titolare della manutenzione HW e SW	M
	4	1	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Non implementato	S
		2	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Non implementato	S
		3	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Non implementato	S
	5	1	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Implementato: gestione della società titolare della manutenzione HW e SW	S
	6	1	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	Non implementato	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Non implementato: attualmente utilizzate password a 6/8 caratteri	M
		2	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Non implementato	S
		3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Non implementato	M
		4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non implementato	M
		5	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Non implementato	S
		6	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Non implementato	S

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

	8	1	Non consentire l’accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un’utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	Non implementato	S

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	9	1	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	Non implementato	S
		1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Implementato: gestione della società titolare della manutenzione HW e SW. Implementato nelle utenze degli applicativi. A livello di server non esiste distinzione	M
		2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Implementato: gestione della società titolare della manutenzione HW e SW	M

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

	10	3	Le utenze amministrative anonime, quali “root” di UNIX o “Administrator” di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l’imputabilità di chi ne fa uso.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		4	Evitare l’uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Implementato: ogni macchina è nel dominio e tutti gli account sono nel dominio.	S
5	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Se per l’autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non implementato: nel caso di ricorso all’autenticazione con certificati digitali, il servizio verrà implementato.	M

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
8	1	1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Implementato: gestione della società titolare della manutenzione HW e SW.	M
		2	Installare su tutti i dispositivi firewall ed IPS personali.	Implementato: gestione della società titolare della manutenzione HW e SW anche se il firewall è periferico, non agisce su ogni dispositivo ma sulla rete globale.	M
		3	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Implementato: gestione della società titolare della manutenzione HW e SW – Log anche su firewall	S
	2	1	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Implementato: gestione della società titolare della manutenzione HW e SW	S
		2	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	Implementato: gestione della società titolare della manutenzione HW e SW	S
		3	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Non implementato.	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
8	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Non implementato	A
	4	1	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Non implementato	S
		2	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Implementato: gestione della società titolare della manutenzione HW e SW mediante tre scansioni	A
	5	1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Implementato: gestione della società titolare della manutenzione HW e SW Per il software esiste un firewall che protegge la rete locale (server e pc) da intrusioni esterne	S
		2	Installare sistemi di analisi avanzata del software sospetto.	Non implementato	A
	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Implementato: gestione della società titolare della manutenzione HW e SW mediante "blocco" di alcuni indirizzi	S
ABSC_ID #			**Descrizione**	**Modalità di Implementazione**	**Liv**

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

8	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Implementato: gestione della società titolare della manutenzione HW e SW. Automaticamente dal S.O. Windows	M
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Implementato: gestione della società titolare della manutenzione HW e SW. Effettuato su file provenienti dall'esterno (es. Internet)	M
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Implementato: gestione della società titolare della manutenzione HW e SW di default	M
		4	Disattivare l'anteprima automatica dei contenuti dei file.	Implementato: gestione della società titolare della manutenzione HW e SW di default	M
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Non implementato	M
	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Implementato: gestione della società titolare della manutenzione HW e SW	M
		2	Filtrare il contenuto del traffico web.	Non implementato. Effettuato in passato ma poi disattivato.	M
		3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Non implementato	M
ABSC_ID #			**Descrizione**	**Modalità di Implementazione**	**Liv**

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

8	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Non implementata la scansione euristica	S
	11	1	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	Non implementata	S

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC 10 (CSC 10): COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Implementato: gestione della società titolare della manutenzione HW e SW quotidianamente. le copie vengono fatte giornalmente su un dispositivo di rete NAS, settimanalmente riversa i dati su un disco esterno. Il disco esterno viene custodito in cassaforte.	M
		2	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Implementato: gestione della società titolare della manutenzione HW e SW. Solo server. Giornalmente viene effettuata la copia delle macchine virtuali.	A
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Non implementato	A
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Implementato: gestione della società titolare della manutenzione HW e SW. Verificato e testato il funzionamento del ripristino macchine virtuali	S
	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Implementato: gestione della società titolare della manutenzione HW e SW. Viene assicurata la protezione fisica. Non si effettua la cifratura dei dati.	M

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Implementato: gestione della società titolare della manutenzione HW e SW. Il disco viene fisicamente distaccato dall'unità.	M

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
13	1	1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Non implementato: non viene effettuata la scrittura crittografica	M
	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Non implementato	S
	3	1	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	Non implementato	A
	4	1	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	Non implementato	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
	5	1	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	Non implementato	A
		2	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	Non implementato dato che non è consentito alcun accesso a dispositivi esterni	A
	6	1	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	Non implementato	A
		2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Non implementato	A
	7	1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Non implementato	A
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	Implementato: gestione della società titolare della manutenzione HW e SW	M

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione

	9	1	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository..	Non implementato	A

Riproduzione cartacea del documento
Registro di Protocollo Generale: 2025 / 3359 del 05/03/2025

copia informatica per consultazione



COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

Proposta N. 2025 / 404
AREA AMMINISTRATIVA

OGGETTO: APPROVAZIONE DOCUMENTO AGGIORNATO "MISURE MINIME DI SICUREZZA ICT" DI CUI ALLA CIRCOLARE AGID N. 2/2017

La presente deliberazione non necessita del parere di regolarità contabile in quanto non comporta riflessi diretti o indiretti né sulla situazione economico-finanziaria né sul patrimonio dell'Ente.

Lì, 07/03/2025

IL DIRIGENTE
SERVIDEI STEFANO
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

copia informatica per consultazione



COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

Proposta N. 2025 / 404
AREA AMMINISTRATIVA

OGGETTO: APPROVAZIONE DOCUMENTO AGGIORNATO "MISURE MINIME DI SICUREZZA ICT" DI CUI ALLA CIRCOLARE AGID N. 2/2017

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

Per i fini previsti dall'art. 49 del D. Lgs 18.08.2000 n° 267, si esprime sulla proposta di deliberazione in oggetto parere FAVOREVOLE in merito alla regolarità tecnica.

Lì, 05/03/2025

IL DIRIGENTE
MAZZANTI AGNESE
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

copia informatica per consultazione

COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

Deliberazione di Giunta Comunale N. 39 del 07/03/2025

ATTESTAZIONE DI PUBBLICAZIONE

Si dichiara la regolare pubblicazione della presente deliberazione all'Albo Pretorio on-line di questo Comune a partire dal 13/03/2025 per 15 giorni consecutivi, ai sensi dell'art. 124 del D.lgs. 18.08.2000 n. 267 e la contestuale comunicazione ai Capigruppo consiliari ai sensi dell'art. 125 del D.lgs. 18.08.2000 n. 267.

Li, 13/03/2025

L'INCARICATO DELLA PUBBLICAZIONE
MAZZANTI AGNESE
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e
s.m.i.)

copia informatica per consultazione



Comune di Campo nell’Elba

Provincia di Livorno

Certificato di Esecutività

Delibera N. 39 del 07/03/2025

AREA AMMINISTRATIVA

Oggetto: APPROVAZIONE DOCUMENTO AGGIORNATO "MISURE MINIME DI SICUREZZA ICT" DI CUI ALLA CIRCOLARE AGID N. 2/2017.

Si attesta che il presente atto sarà pubblicato all’Albo Pretorio per 15 giorni consecutivi, dal 13/03/2025 al 28/03/2025, e che sarà esecutivo in data 24/03/2025.

Campo nell’Elba li, 24/03/2025

IL RESPONSABILE DEL SETTORE
MAZZANTI AGNESE
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

copia informatica per consultazione

Soggetto	Denominazione corso (tipologia e livello)	Programmazione (date)
Nuovi dipendenti	Formazione Privacy 2024 - Corso base per nuovi dipendenti - parte 1-2	31/12/2025
Nuovi dipendenti	Formazione Privacy 2024 - Corso base per nuovi dipendenti - parte 3-4	31/12/2025
Tutti i dipendenti	Formazione Privacy 2024 - Corso generale di aggiornamento	31/12/2025
Dipendenti del Servizio/Ufficio	Formazione Privacy 2024 - Corso n. 1 - Corso servizi Demografici	31/12/2025
Dipendenti del Servizio/Ufficio	Formazione Privacy 2024 - Corso n. 2 - Corso servizi Sociali	31/12/2025
Dipendenti del Servizio/Ufficio	Formazione Privacy 2024 - Corso n. 3 - Corso Segreteria Affari Generali e Ufficio del Personale	31/12/2025
Dipendenti del Servizio/Ufficio	Formazione Privacy 2024 - Corso n. 4 - Corso Ufficio Responsabile Transizione al Digitale (CED) - Servizi Informatici	31/12/2025
Dipendenti del Servizio/Ufficio	Formazione Privacy 2024 - Corso n. 5 - Corso Ufficio Tecnico ed Ufficio Ambiente	31/12/2025
Dipendenti del Servizio/Ufficio	Formazione Privacy 2024 - Corso n. 6 - Corso Servizi finanziari Ragioneria ed Ufficio Tributi	31/12/2025
Dipendenti del Servizio/Ufficio	Formazione Privacy 2024 - Corso n. 7 - Corso Polizia Locale	31/12/2025
Amministratori	Formazione Privacy 2024 - Corso n. 8 - Corso Amministratori	31/12/2025

copia informatica per consultazione

COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

Proposta N. 2025 / 614
SERVIZIO SEGRETERIA, PROTOCOLLO E SERV. NOTIIFICA, UFF. PERSONALE

OGGETTO: APPROVAZIONE DEL PIANO DI PROTEZIONE DEI DATI PERSONALI E DI GESTIONE DEL RISCHIO DI VIOLAZIONE

La presente deliberazione non necessita del parere di regolarità contabile in quanto non comporta riflessi diretti o indiretti né sulla situazione economico-finanziaria né sul patrimonio dell'Ente.

Lì, 03/04/2025

IL DIRIGENTE
SERVIDEI STEFANO
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

copia informatica per consultazione

COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

Proposta N. 2025 / 614
SERVIZIO SEGRETERIA, PROTOCOLLO E SERV. NOTIIFICA, UFF. PERSONALE

OGGETTO: APPROVAZIONE DEL PIANO DI PROTEZIONE DEI DATI PERSONALI E DI GESTIONE DEL RISCHIO DI VIOLAZIONE

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

Per i fini previsti dall'art. 49 del D. Lgs 18.08.2000 n° 267, si esprime sulla proposta di deliberazione in oggetto parere FAVOREVOLE in merito alla regolarità tecnica.

Lì, 03/04/2025

IL DIRIGENTE
MAZZANTI AGNESE
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

copia informatica per consultazione

COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno
******

Deliberazione di Giunta Comunale N. 70 del 04/04/2025

ATTESTAZIONE DI PUBBLICAZIONE

Si dichiara la regolare pubblicazione della presente deliberazione all'Albo Pretorio on-line di questo Comune a partire dal 10/04/2025 per 15 giorni consecutivi, ai sensi dell'art. 124 del D.lgs. 18.08.2000 n. 267 e la contestuale comunicazione ai Capigruppo consiliari ai sensi dell'art. 125 del D.lgs. 18.08.2000 n. 267.

Li, 10/04/2025

L'INCARICATO DELLA PUBBLICAZIONE
MAZZANTI AGNESE
(Sottoscritto digitalmente
ai sensi dell'art. 21 D.L.gs. n. 82/2005 e
s.m.i.)

copia informatica per consultazione



Comune di Campo nell’Elba

Provincia di Livorno

Certificato di Esecutività

Delibera N. 70 del 04/04/2025

AREA AMMINISTRATIVA

Oggetto: APPROVAZIONE DEL PIANO DI PROTEZIONE DEI DATI PERSONALI E DI GESTIONE DEL RISCHIO DI VIOLAZIONE.

Si attesta che il presente atto sarà pubblicato all’Albo Pretorio per 15 giorni consecutivi, dal 10/04/2025 al 25/04/2025, e che sarà esecutivo in data 21/04/2025.

Campo nell’Elba li, 23/04/2025

IL RESPONSABILE DEL SETTORE
MAZZANTI AGNESE
(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)

copia informatica per consultazione