DPIA uso Fototrappole e telecamere ZTL

AUTORE : Isp. Francesco MODICA DI MARCO

REVISORE: Avv. Guido PARATICO

VALIDATORE : Isp. Francesco MODICA DI MARCO

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Questa DPIA è atta alla valutazione dell'impatto connesso all'uso di nuove tecnologie al fine di rilevare immagini catturate attraverso l'utilizzo di fototrappole e telecamere fisse per poi poter comminare sanzioni amministrative contro l'abbandono incontrollato dei rifiuti sul suolo nel territorio del Comune di Campo nell'Elba e per l'illecito passaggio non autorizzato nelle Zone a Traffico Limitato nella frazione di Marina di Campo. Nel presente DPIA sono presi in considerazione i trattamenti dei dati personali operati per mezzo di tecnologie che permettono le rivelazioni di filmati e immagini degli interessati nonchè i numeri delle targhe dei veicoli transitanti le zone videosorvegliate nel territorio comunale.

Quali sono le responsabilità connesse al trattamento?

Il titolare del trattamento dei dati è il Comune di Campo nell'Elba, rappresentato, ai fini previsti dal G.D.P.R., dal Sindaco pro tempore.
Il titolare è responsabile dell'osservanza dei principi applicabili al trattamento di dati personali stabiliti dall'articolo 5 del G.D.P.R.: Liceità, correttezza e trasparenza, limitazione della finalità, minizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza. Il titolare mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento di dati personali è effettuato in modo conforme al G.D.P.R. Le misure sono definite fin dalla fase di progettaione e messe in atto per applicare in mnodo efficace i principi di protezine dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del G.D.P.R. nonchè le cominucazioni e le informazioni occorrenti per il loro esercizio.Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei corsi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Il titolare adotta misure appropriate per fornire all'interessato:

1. le informazioni indicate dall'articolo 13 G.D.P.R., qualora i dati personali siano raccolti presso lo stesso interessato;
2. le informazioni indicate dall'articolo 14 G.D.P.R., qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologia, possa presentare un rischio elevato per i diritti e le liberrtà delle persone fisiche, il titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (D.P.I.A.) ai sensi dell'articolo 35 G.D.P.R., considerando la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.
il titolare, inoltre, provvede a:

- designare i delegati al trattamento nelle figure dei Responsabili PO e dei funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;
- nominare il Responsabile della Protezione dei Dati;
- nominare eventuale quale responsabile del trattamento esterno soggetti pubblici e privati affidatari di attività e servizi per conto dell'Amministrazione Comunale anche relativamente alle banche dati gestiti da soggetti esterni al Comune in virtù di convenzioni, contratti, incarichi professinali o altri strumenti guiridici consenttiti dalla Legge per la realizzazione di attività connesse per scopi istituzionali.

Il delegato interno al trattamento viene individuato nella figura del Responsabile della Polizia Municipale del Comune di Campo nell'Elba. Il Delegato al trattamento provvede per il proprio ambito di competenza a tutte le attività previste dalla Legge e a tutti i compiti a lui affidati dal Titolare individuati nell'atto di designazione con Decreto del Sindaco.
Il delegato al trattamento può altresì designare altri soggetti incaricati al rattamento dei dati personali identificandoli tra i collaboratori presso la struttura organizzativa all'interno della Polizia Municipale.

Ci sono standard applicabili al trattamento?

Attualmente non sono stati rinvenuti standard, certificazioni o codici di condotta applicabili al problema in esame.

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Filmati, immagini che ritraggono persone fisiche e/o numeri di targa di veicoli transitanti nelle zone videosorvegliate allo scopo di controllare i passaggi illeciti nelle ZTL e gli abbandoni incontrollati dei rifiuti e altri tipi di illeciti di tipo amministrativo sul territorio del Comune di Campo nell'Elba. I dati verranno conservati per il periodo necessario alla comminazione delle relative ed eventuali sanzioni amministrative, nonchè in conformità alla normativa vigente in materia di accesso agli atti.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Le telecamere sui varchi in entrata ed in uscita dalle Zone a Traffico Limitato sono omologate con decreto dirigenziale (prot. 2849 del 17/05/2014), i segnali vengono trasmessi tramite rete ethernet

collegata direttamente alle telecamere. Ogni singola immagine rilevata, in entrata ed in uscita dai varchi, viene abbinata automaticamente dalla telecamera OCR alla lettura della targa ed ogni fotogramma riporta indicazioni riguardanti orario dell'avvenuto passaggio, luogo di rilevamento e nominativo del varco. Il sistema consente di rilevare il numero dei veicoli transitati da ogni varco e il numero totale di quelli in infrazione per passaggio non autorizzato. L'impianto è mantenibile da remoto con accesso protetto tramite Password e registrazione dell'utente e delle attività effettuate. Il server centrale per la raccolta dei dati provvede al continuo monitoraggio delle postazioni di interfaccia locale. Sul Server saranno raccolti periodicamente tutti gli archivi contenenti le immagini delle targhe rilevate e non autorizate al transito. Sono memorizzati tutti i "report" relativi a qualunque modifica effettuata verso l'unità di ripresa, questa funzione consente un controllo puntuale e preciso evitando l'insorgere di alcun dubbio sulla gestione dell'impianto da parte di chi ha accesso al sistema, compreso i tecnici autorizzati agli interventi manutentivi.
Tutta la comunicazione avviene in modo criptato e su linee telefoniche commutate o dedicate, o su linee di comunicazione ethernet. I dati sul server vengono memorizzati mediante l'utilizzo di un gestore di data-base relazionale che garantisce l'integrità e la ridondanza dei dati, questi vengono, infatti, duplicati su dischi separati in modo completamente automatico (mirroring). Il server permette, inoltre, diversi livelli di accesso alle informazioni ed alle immagini a tutti i client abilitati alla gestione. Ogni utente viene identificato al momento del collegamento con un profilo in base al quale vengono abilitati i diversi livelli di accesso alle procedure ed ai dati. Le immagini salvate sul server sono visionate e i dati personali trattati allo scopo sanzionatorio, esclusivamente da soggetti autorizzati dal Responsabile del trattamento dei dati. Il ciclo di vita dei dati e delle immagini segue il periodo di legge previsto per l'iter sanzionatorio e quale indicato dalla norma relativa all'accesso agli atti. Le immagini e i dati che non servono allo scopo previsto dal sistema in oggetto e disciplinato dal presente DPIA, vengono scartate ed eliminate.
Le fototrappole vengono collocate nelle zone debitamente segnalate, con cartelli indicanti la zona controllata da telecamere. Ogni immagine criptata viene scaricata dalla telecamera sulla postazione PC dedicata per mezzo di un software e salvata. L'utilizzo e l'accesso ai dati, nonchè la gestione della stessa fototrappola, viene affidata a personale dell'ufficio di Polizia Municipale di Campo nell'Elba, debitamente formato e autorizzato. Le immagini rilevate vengono conservate per i soli scopi sanzionatori in occasione di illeciti relativi all'abbandono incontrollato di rifiuti o di altro comportamento in violazione di regolamenti comunali o Leggi regionali o Statali in materia di illeciti amministrativi. I dati e le immagini che non producono effetti giuridici vengono cancellate dalla memoria della telecamera stessa e non vengono neanche scaricati sulla postazione PC dedicata. I rilevamenti che hanno dato luogo al procedimento sanzionatorio vengono conservati per il periodo di legge previsto all'iter sanzionatorio amministrativo e per l'esercizio del diritto di accesso agli atti previsto dalla Legge in materia. La fototrappola è protetta da custodia in acciaio inox e lucchetto per garantirne l'integrità e impedire le eventuali manomissioni in fase di accertamento.
La visione di ogni dato e di ogni immagine rilevata è consentita al solo personale autorizzato dal Responsabile del trattamento dei dati.

Quali sono le risorse di supporto ai dati?

Ogni dato criptato proveniente dai rilievi effettuati dalle telecamere nei varchi ZTL, viene salvato su un SERVER ubicato presso la sede dell'ufficio di Polizia Municipale permettendo l'analisi e l'elaborazione delle eventuali sanzioni amministrative, nonchè la condivisione per l'organizzazione interna dei compiti assegnati al personale autorizzato.
Per quanto riguarda la conservazione delle immagini e dei dati relativi ai rilievi effettuati con la fototrappola, viene utilizzato il sistema di memoria della postazione PC dedicata, ubicata all'interno dell'ufficio di Polizia Municipale, permettendo l'analisi e l'elaborazione delle eventuali sanzioni, nonchè la condivisione interna dei compiti assegnati al personale autorizzato.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

L'abbandono dei rifiuti incontrollato, la prevenzione di comportamenti in violazione di legge in genere e la vigilanza sugli accessi alle ZTL rappresentano un interesse legato alla collettività ai fini della civile convivenza e tutela del territorio.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento eseguito con le fototrappole, ai sensi dell'articolo 6 comma 1, lettera "e" del Regolamento UE 2016/679, è rapprsentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento. Per l'utilizzo delle telecamere nei varchi delle Zone a Traffico Limitate, si fa riferimento ai poteri demandati ai proprietari della strada, come indicato dalle norme contenute nel Codice della Strada.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati personali acquisiti dalle telecamere nei varchi ZTL e dalle fototrappole vengono elaborati al solo scopo dell'accertamento di eventuali violazioni di tipo amministrativo a normative regionali e Regolamenti Comunali, mediante l'individuazione dei responsabili, attraverso la visione delle immagini, al solo scopo di procedere alla contestazione ed alla notifica del successivo eventuale verbale amministrativo.

I dati sono esatti e aggiornati?

Ogni dato acquisito viene revisionato allo scopo di omettere ogni tipo di errore di lettura delle immagini e dei filmati. gli strumenti tecnologici utilizzati sono regolarmente e costantemente aggiornati nei loro sistemi operativi.

Qual è il periodo di conservazione dei dati?

I dati acquisiti, mediante l'analisi e la visione dei filmati e delle fotografie rilevate dalle telecametre sui varchi ZTL e dalle fototrappole, vengono conservati per il periodo di legge stabilito necessario per la notificazione delle successive sanzioni amministrative e per l'esercizio previsto dalla legge in materia di accesso agli atti .

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono messi a conoscenza dell'utilizzo di fototrappole e telecamere nelle aree del Comune interessate attraverso l'affissione di cartelli di avviso nonchè attraverso un informativa pubblicitaria sul sito istituzionale dell'Ente.

Ove applicabile: come si ottiene il consenso degli interessati?

Non è previsto il preventivo consenso degli interessati, in quanto l'utilizzo dei mezzi di videosorveglianza trattati dal presente DPIA è disciplinato da normative vigenti che ne prevedono l'esonero.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Il diritto di accesso ai dati elaborati, riferiti agli interessati e alla comunità, viene esercitato a seguito di informativa contenuta negli atti notificati, sul sito istituzionale e sui cartelli di avviso delle zone videosorvegliate , come previsto dalla normativa per il diritto di accesso agli atti amministrativi.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

all'interessato, relativamente al trattamento dei suoi dati personali, sono riconosciuti i seguenti diritti:

- richiedere maggiori informazioni in relazione ai contenuti dei verbali amministrativi;
- diritto di accesso ai dati personali (art.15 GDPR);
- diritto di rettifica dei dati personali senza ingiustificato ritardo (art.16 GDPR);
- diritto alla cancellazione dei dati. La cancellazione non è consentita per i dati contenuti negli atti che devono obbligatoriamente essere conservati dal Titole (art.17 GDPR);
- diritto di limitazione del trattamento (art.18 GDPR);
- diritto alla portabilità dei dati (art.20 GDPR);
- diritto di opposizione (art.21 GDPR);
- diritto relativo al processo decisionale automatizzato, compresa la profilazione (art.22 GDPR);
- diritto di proporre reclamo al Garante per la protezione dei dati personali (art.77 GDPR);

Ogni interessato ha la facoltà di far valere i propri diritti riconosciuti dalla Legge attraverso i sistemi indicati sugli atti notificati, di cui risulta intestatario, sui cartelli indicanti le zone videosorvegliate e sul sito istituzionale del Comune di Campo nell'Elba.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

all'interessato viene garantito il diritto alla limitazione del trattamento dei dati (art.18 del GDPR) e all'opposizione (art.21 del GDPR), attraverso i sistemi indicati sugli atti notificati di cui risulta intestatario, sui cartelli indicanti le zone videosorvegliate e sul sito istituzionale del Comune di Campo nell'Elba.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi del responsabile del Trattamento dei dati sono dettati nel Decreto di nomina del Sindaco di Campo nell'Elba e dai contratti e le convenzioni con i concessionari per la gestione del ciclo contravvenzionale.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Gli atti amministrativi relativi alle violazioni da parte di cittadini residenti fuori dall'UE vengono trattati con la medesima protezione di quelli residenti all'interno della UE.

Rischi

Misure esistenti o pianificate

Controllo degli accessi logici

l'accesso agli strumenti informatici avviene tramite l'utilizzo di password alfanumeriche che vengono modificate periodicamente al fine di garantire un accesso sicuro.

Archiviazione

la documentazione digitale relativa all'attività di rilevazione delle immagini e dei filmati viene salvata su server e su postazioni PC dedicate e regolamentata dalla normativa vigente in materia di archiviazione nella Pubblica Amministrazione.

Sicurezza dei documenti cartacei

i documenti cartacei vengono conservati e archiviati nei locali indisponibili all'utenza dell'ufficio di Polizia Municipale e quelli inutilizzabili vengono distrutti con appositi macchinari tritacarte.

Vulnerabilità

i software utilizzati per la trasmissione dei dati sono costantemente aggiornati. I filmati e le immagini possono essere visionati solo con l'ausilio di un software licenziato e le apparecchiature sono soggette a revisione periodica.

Lotta contro il malware

i sistemi informatici sono protetti dal malware con modalità di protezione sia hardware che software (antivirus).

Gestione postazioni

la postazione presente presso l'ufficio di Polizia Municipale è dotata di PC con relativa password alfanumerica che viene modificata periodicamente al fine di garantire un accesso sicuro.

Backup

il backup dei dati trattati avviene periodicamente ed in modo automatico su disco fisso.

Manutenzione

la manutenzione dei sistemi è stata affidata a Ditta specializzata tramite affidamento effettuato a norma di legge.

Controllo degli accessi fisici

l'accesso al server è consentito solo al personale autorizzato.

Sicurezza dell'hardware

il server è ubicato presso i locali indisponibili all'utenza dell'ufficio di Polizia municipale e l'accesso è consentito esclusivamente al personale autorizzato.

Politica di tutela della privacy

L'Amministrazione ha messo in atto una serie di misure orientate all'adeguamento della normativa vigente nominando i dipendenti autorizzati al trattamento dei dati, ai sensi dell'articolo 2.quaterdecies del D.Lgs. 196/2003.

Gestione delle politiche di tutela della privacy

L'Ente è dotato di linee guida per l'attuazione degli obblighi introdotti dal reg. UE 679/2016 nonchè di linee guida sulla politica per la sicurezza, l'utilizzo di strumenti informatici, posta elettronica e internet.

Crittografia

Ogni immagine rilevata dai sitemi di videosorveglianza è criptata e scaricata su un server o su un pc dedicato da personale della Polizia Municipale di Campo nell'Elba debitamente formato ed autorizzato.

Rischi

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

violazione delle norme sulla riservatezza dei dati personali comuni e/o sensibili.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

accesso abusivo ai sistemi.

Quali sono le fonti di rischio?

il soggetto autorizzato che si renda responsabile per negligenza di un possibile accesso da parte di personale non autorizzato

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Sicurezza dei documenti cartacei, Gestione postazioni, Lotta contro il malware, Manutenzione, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Archiviazione, Vulnerabilità, Gestione delle politiche di tutela della privacy, Crittografia

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, limitata.
L'accesso ai locali dell'ufficio di Polizia Municipale è consentito esclusivamente al personale autorizzato, debitamente formato e reso edotto delle responsabilità inerenti alla divulgazione dei dati personali. Le Password per accedere ai sistemi sono periodicamente aggiornate.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, limitato

Rischi

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

violazione delle norme sulla riservatezza dei dati personali comuni e/o sensibili.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

accesso abusivo ai sistemi.

Quali sono le fonti di rischio?

il soggetto autorizzato che si renda responsabile per negligenza di un possibile accesso da parte di personale non autorizzato

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Sicurezza dei documenti cartacei, Lotta contro il malware, Gestione postazioni, Manutenzione, Sicurezza dell'hardware, Controllo degli accessi fisici, Politica di tutela della privacy, Archiviazione, Vulnerabilità, Gestione delle politiche di tutela della privacy, Crittografia

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata, limitato.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile, trascurabile.

Rischi

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

violazione delle norme sulla riservatezza dei dati personali comuni e/o sensibili.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

accesso abusivo ai sistemi.

Quali sono le fonti di rischio?

il soggetto autorizzato che si renda responsabile per negligenza di un possibile accesso da parte di personale non autorizzato

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Manutenzione, Controllo degli accessi fisici, Sicurezza

dell'hardware, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Crittografia

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

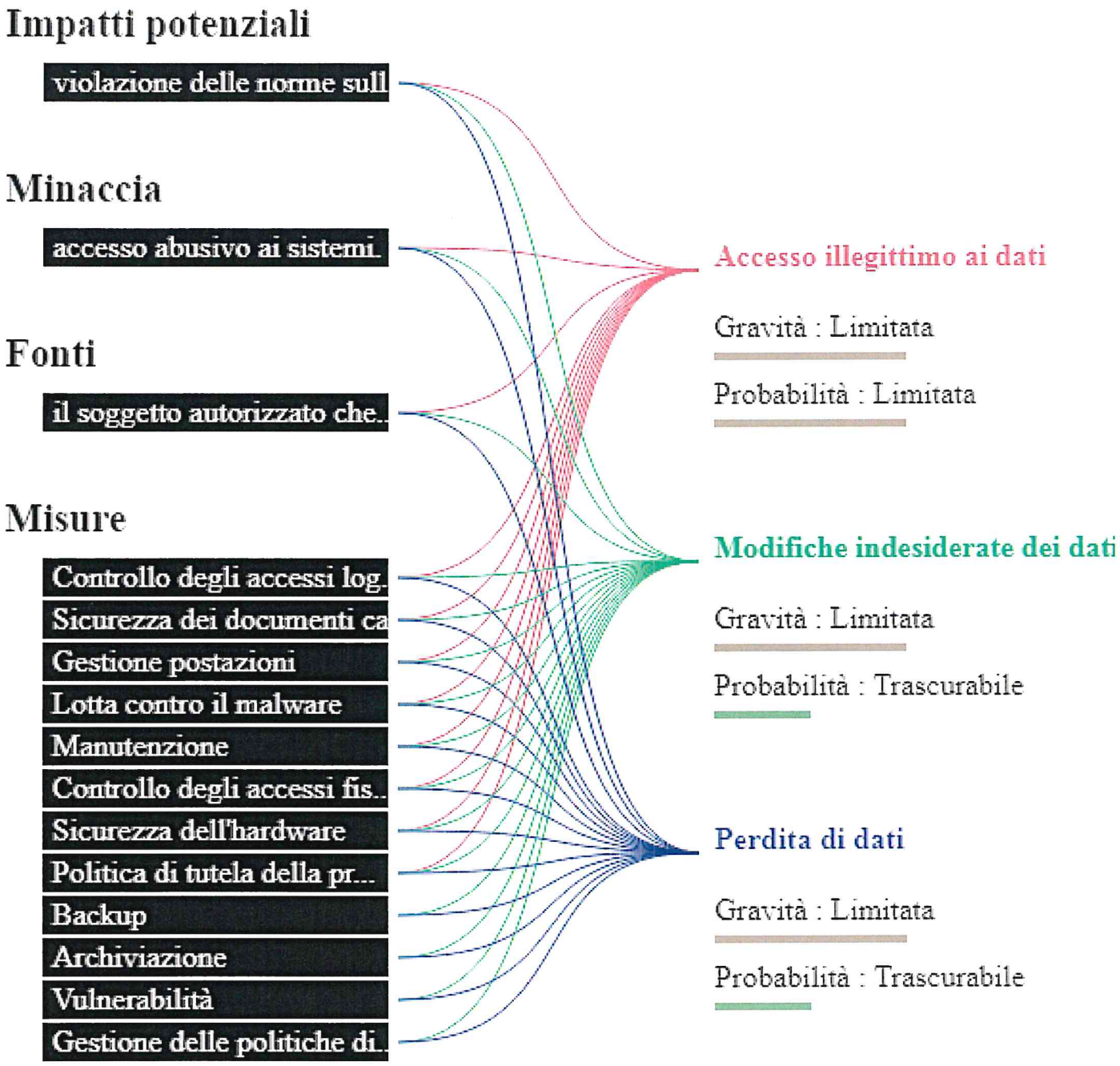
Limitata, limitato

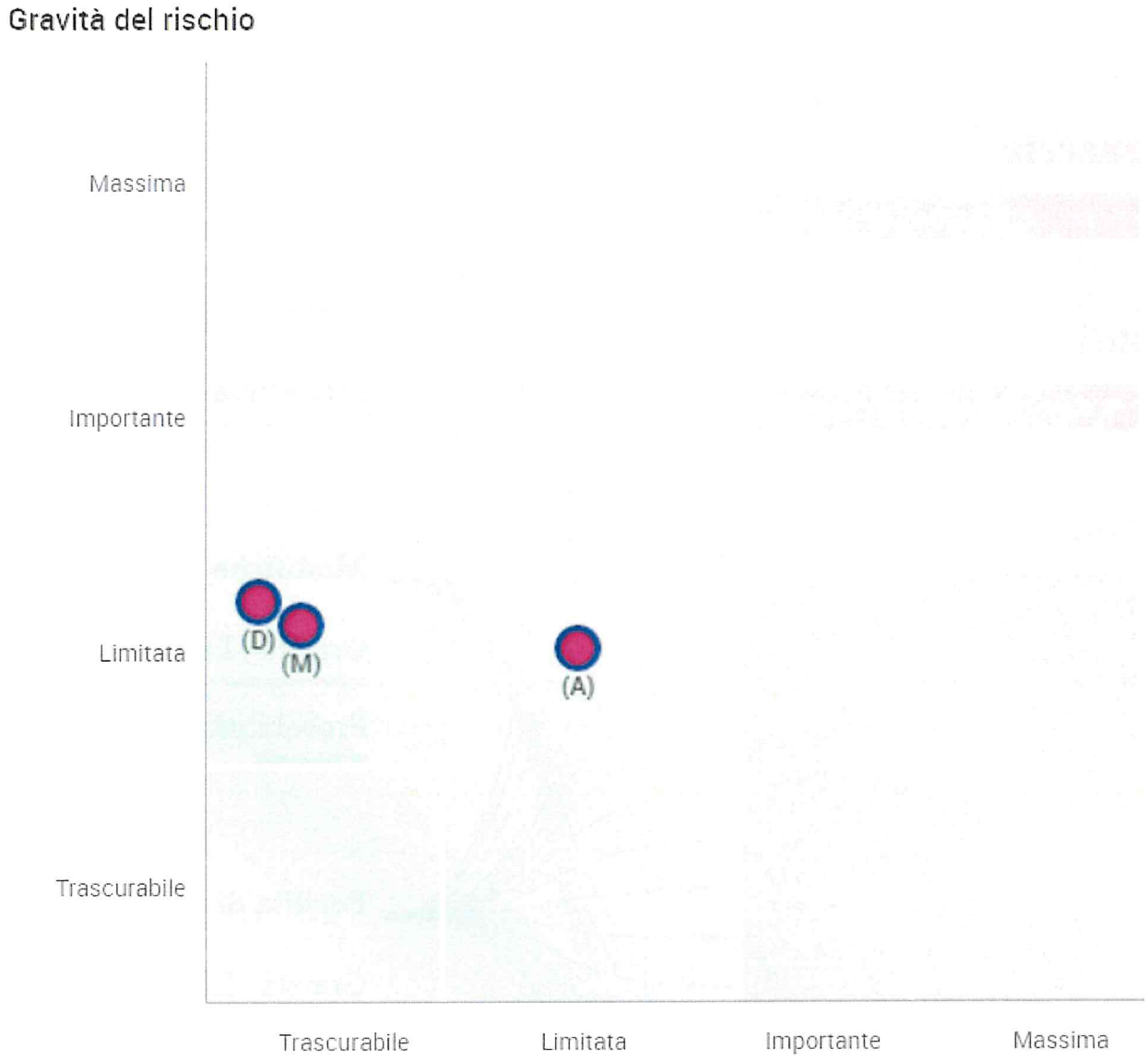
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, trascurabile

Rischi

Panoramica dei rischi


Impatti potenziali
violazione delle norme sull
Minaccia
accesso abusivo ai sistemi
Fonti
il soggetto autorizzato che..
Misure
Controllo degli accessi log..
Sicurezza dei documenti ca
Gestione postazioni
Lotta contro il malware
Manutenzione
Controllo degli accessi fis..
Sicurezza dell'hardware
Politica di tutela della pr...
Backup
Archiviazione
Vulnerabilità
Gestione delle politiche di..
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Limitata
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Trascurabile



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Panoramica

Principi fondamentali

Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Informativa
Raccolta del consenso
Diritto di accesso e diritto alla portabilità dei dati
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione
Responsabili del trattamento
Trasferimenti di dati

Misure esistenti o pianificate

Controllo degli accessi logici
Archiviazione
Sicurezza dei documenti cartacei
Vulnerabilità
Lotta contro il malware
Gestione postazioni
Backup
Manutenzione
Controllo degli accessi fisici
Sicurezza dell'hardware
Politica di tutela della privacy
Gestione delle politiche di tutela della privacy

Rischi

Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure Migliorabili
Misure Accettabili