Informazioni sulla PIA

Nome della PIA
DPIA Videosorveglianza e fototrappolaggio

Nome autore
Sindaco

Nome valutatore
Segretario Generale

Nome validatore
Responsabile Protezione Dati

Data di creazione
21/01/2020

Nome del DPO/RPD
Simone Carmignani

Parere del DPO/RPD
Il trattamento può essere implementatoper le motivazioni e le finalità che sono alla base del trattamento stesso.

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Il numero degli interessati è eccessivamente elevato per poter chiedere singolarmente il parere, è stato tuttavia pubblicato sul sito web dell'ente il regolamento specifico che disciplina il servizio e gli avvisi pubblici di implementazione dello stesso.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento operato dagli agenti di Polizia Locale, interamente o parzialmente automatizzato, dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio attivati nel territorio dell'Ente, ai sensi del Reg. UE 2016/679, della Direttiva UE 2016/680, in osservanza delle disposizioni contenuti nel "decalogo" del 8 aprile 2010 dal Garante della Privacy e del Codice Nazionale sulla Privacy dlgs 196/2003.

L'impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati e ha come obbiettivo di verificare e garantire la protezione dei dati personali di tutti coloro che entrano in contatto o in relazione con l'attività di videosorveglianza e fototrappolaggio.

L'utilizzo degli impianti è finalizzato a:

a. Attività di prevenzione, indagine, accertamento e perseguimento di atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 e s.m.i., delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del dlgs 267/2000;

b. Prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado, di discarica di materiale e di sostanze pericolose o di abbandono di rifiuti, e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nel regolamento di polizia urbana, nei Regolamenti locali in genere e nelle Ordinanze Sindacali;

c. Vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;

d. Tutelare l'ordine, il decoro e la quiete pubblica;

e. Controllare aree specifiche del territorio comunale;

f. Monitorare e controllare la viabilità e i flussi di traffico;

g. Verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici;

h. Coordinamento delle attività di protezione civile.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità del trattamento sono connesse ai ruoli ricoperti, il titolare del trattamento è il Sindaco pro tempore, il designato al trattamento (responsabili interni) è il dirigente/responsabile di posizione organizzativa del servizio di Polizia Locale, se formalmente nominato, possono essere nominati come responsabili esterni del trattamento tutti i soggetti fisici o giuridici che gestiscono per conto dell'ente dati personali nell'ambito di un appalto di servizi relativo al supporto per la gestione degli impianti.

Ci sono standard applicabili al trattamento?

Al momento non sono contemplati standard da applicare direttamente al trattamento, tuttavia l'attività di videosorveglianza e trappolaggio è disciplinata da specifico regolamento dell'ente.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Gli impianti riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese, consentono riprese unicamente di video o foto e sono installati nel territorio dell'Ente e possono essere sia fissi che mobili.

I dati che vengono trattati fanno riferimento a persone fisiche e sono identificativi, relativi al possesso di benie proprietà, caratteristiche fisiche, abitudini, stile vita, comportamento, posizione geografica, immaginie suoni.

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

Il ciclo di vita dei dati prevede i seguenti trattamenti acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione.

Quali sono le risorse di supporto ai dati?

Gli impianti consentono riprese video e foto a colori, diurne e notturne, in condizioni di sufficiente illuminazione naturale o artificiale, gli impianti di videosorveglianza sono sempre in funzione e registrano in maniera continuativa, mentre gli impianti di fototrappolaggio si innescano in modo autonomo a seguito di qualsiasi movimento di veicoli o esseri umani catturando immagini.
I segnali video e foto delle unità di ripresa sono inviati presso la sede comunale o data center individuato appositamente dove sono registrati su appositi server. In queste sedi le immagini sono visualizzate su monitor e hardware client appositamente configurato il cui accesso è protetto, riservato e consentito unicamente al personale formalmente e appositamente incaricato.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali, acquisiti mediante l'utilizzo degli impianti di videosorveglianza e di fototrappolaggio gestiti dall'Ente e collegati alle centrali di controllo ubicate presso gli Uffici dell'Ente, si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce al contempo il rispetto dei diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.

L'utilizzo degli impianti comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese video e foto che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area oggetto di sorveglianza.

Il trattamento dei dati personali si svolge nel pieno rispetto dei principi di liceità, finalità, limitazione pertinenza e proporzionalità, sanciti dal Codice Privacy novellato e dal Reg. UE2016/679.

In attuazione dei principi di liceità e finalità, il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza è effettuato dall'Ente esclusivamente per lo svolgimento delle funzioni istituzionali .

In attuazione del principio di limitazione e pertinenza, gli impianti di videosorveglianza, fototrappolaggio e i programmi informatici di gestione sono configurati in modo da ridurre al minimo l'uso di dati personali ed identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi o con modalità che permettano di identificare l'interessato solo in caso di necessità, sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Valutazione : Accettabile

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 raccolti ed elaborati vengono costantemente minimizzati utilizzando unicamente le informazioni strettamente necessarie all'erogazione del servizio, viene praticata la limitazione dei dati soprattutto in

relazione agli obblighi di pubblicazione.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati vengono aggiornati periodicamente, almeno su base annuale, e incrociati con le banche dati nazionali.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono cancellati con modalità automatica. Gli strumenti e i supporti elettronici utilizzati sono dotati dei sistemi di protezioni che garantiscono la tutela dei dati trattati.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

L'informativa sul trattamento dei dati viene sempre resa a tutti gli interessati sia in modalità telematica che cartacea, è poi pubblicata sul sito web ufficiale dell'ente l'informativa estesa che piega anche nel dettaglio l'utilizzo dei cookie.
In particolare sono affissi nel territorio comunale i cartelli relativi allo svolgimento dell'attività di videosorveglianza e trappolaggio.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Essendo l'ente una pubblica amministrazione che eroga servizi pubblici legalmente attribuiti non è tenuto all'acquisizione del consenso al trattamento dei dati, nei casi in cui questo sia dovuto viene acquisito per iscritto.

Valutazione : Accettabile

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

In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:

a. Di ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;

b. Di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;

c. Di richiedere su richiesta avanzata prima dello spirare del termine massimo di conservazione del dato e di ottenere, senza ritardo e comunque non oltre 30 giorni dal

responsabile designato:

- La conferma dell'esistenza o meno di dati personali che lo riguardano, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento;
- La cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati, valutate le preminenti esigenze di polizia giudiziaria e di indagine.

d. Di opporsi, in tutto o in parte, per motivi legittimi qualora sia possibile, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

Nell'esercizio dei suoi diritti l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.

Le istanze di cui al presente articolo possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata o posta elettronica certificata, nel caso di esito negativo alla istanza l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Possono essere adottate misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:

a.1. Non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

b.2. Non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;

c.3. Proteggere la sicurezza pubblica;

d.4. Proteggere la sicurezza nazionale;

e.5. Proteggere i diritti e le libertà altrui.

Valutazione : Accettabile

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

Per esercitare il diritto alla cancellazione, se possibile in ragione dell'obbligo dell'ente di conservazione delle informazioni, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

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

Per esercitare il diritto di limitazione o oppoesizione, se possibile, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

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

Gli obblighi di ogni singolo responsabile del trattamento sono definiti nei contratti di appalto dei relativi servizi o con specifica comunicazione.

Valutazione : Accettabile

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

I dati non vengono trasferiti al di fuori dell'Unione Europea.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Anonimizzazione

I particolari tipi di dati, ovvero i c.d. dati sensibili, vengono trattati in maniera riservata unicamente dal personale strettamente necessario e a questo autorizzato, vengono resi sempre completamente anonimi quando pubblicati.

Valutazione : Accettabile

Controllo degli accessi logici

Ogni operatore una postazione fisica assegnata con cassetti muniti di chiavi se previsti e una postazione informatica dedicata dotata di password univoca di accesso.

Valutazione : Accettabile

Tracciabilità

I flussi documentali interni avvengono tramite posta elettronica oppure attraverso il sistema di comunicazione interno utilizzando il gestionale, entrambe i sistemi lasciano traccia del flusso, tutte le comunicazioni ufficiali all'esterno avvengono invece per mail, pec o raccomandata.

Valutazione : Accettabile

Archiviazione

Ogni responsabile controlla l'archiviazione dei dati gestiti dall'ufficio in una cartella non condivisa su una postazione informatica protetta da password, mentre gli archivi generali dell'ente sono conservati su un server dedicato il cui accesso è limitato e controllato. Per quanto riguarda l'archiviazione cartacea questa avviene all'interno degli uffici che trattano i dati e viene garantito l'anonimato delle informazioni contenute, per quanto riguarda i particolari tipi di dati vengono previste delle misure di protezione ulteriori e specifiche come armadietti con chiusura a chiave o casseforti.

Valutazione : Accettabile

Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dai dipendenti dell'ufficio, il responsabile verifica che siano disposti in specifici raccoglitori in moda tale che non vadano dispersi e che non siano visibili a terzi non autorizzati, gli uffici devono essere chiusi e l'accesso consentito soltanto agli addetti o ai soggetti autorizzati.

Valutazione : Accettabile

Minimizzazione dei dati

Vengono raccolti e conservati unicamente i dati necessari all'erogazione del servizio.

Valutazione : Accettabile

Vulnerabilità

I software in uso vengono aggiornati costantemente e l’accesso ai dati è limitato unicamente agli operatori direttamente interessati ai quali viene assegnato un account univoco e tracciabile.

Valutazione : Accettabile

Lotta contro il malware

L’antimalware è regolarmente istallato e costantemente aggiornato.

Valutazione : Accettabile

Backup

I backup vengono regolarmente effettuati.

Valutazione : Accettabile

Manutenzione

La manutenzione fisica dei dispositivi viene effettuata all’occorrenza.

Valutazione : Accettabile

Sicurezza dei canali informatici

Il firewall risulta regolarmente istallato e costantemente aggiornato.

Valutazione : Accettabile

Controllo degli accessi fisici

Gli accessi fisici agli uffici sono limitati e controllati.

Valutazione : Accettabile

Sicurezza dell'hardware

L’accesso alla rete informatica interna è limitato, viene protetto da account e password personali.

Valutazione : Accettabile

Prevenzione delle fonti di rischio

Gli uffici dell’ente risultano rispettare le previsioni normative in materia di salute e protezione sui luoghi di lavoro.

Valutazione : Accettabile

Politica di tutela della privacy

È stato regolarmente incaricato il responsabile della protezione dei dati e la nomina comunicata al garante sulla protezione dei dati.

Valutazione : Accettabile

Gestione dei rischi

Sono stati redatti e approvati i registri sul trattamento, la valutazione e l'impatto sui dati personali.

Valutazione : Accettabile

Gestione del personale

I dipendenti sono regolarmente invitati a partecipare alle giornate di aggiornamento e formazione, una volta che cessa il rapporto di lavoro vengono cambiati gli identificativi di accesso e le password.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

I collaboratori e i partner esterni sono sottoposti alle stesse regole e controlli del personale dipendente per l'accesso ai dati.

Valutazione : Accettabile

Specifiche misure di sicurezza

1. Ai sensi di quanto previsto dall'articolo 24 del Reg. UE 2016/679, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di cui all'articolo 3 del presente Regolamento.
2. Ai sensi dell'art. 29 c. 2 della Direttiva UE 2016/680 il Titolare del trattamento, previa valutazione dei rischi, mette in atto misure volte a:
    a. Vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);
    b. Impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
    c. Impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);
    d. Impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo

dell'utente»);

e. Garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

f. Garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);

g. Garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

h. Impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);

i. Garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);

j. Garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Valutazione : Accettabile

Accesso illegittimo ai dati

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

Impatto limitato, Impatto significativo

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Perdita di dati, uso improprio di dati, diffusione di dati riservati o sensibili.

Quali sono le fonti di rischio?

Fonti di rischio interne ed esterne anche non umane.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Minimizzazione dei dati, Lotta contro il malware, Backup, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione del personale, Gestione dei terzi che accedono ai dati

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

Importante, il rischio è trascurabile o limitato

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

Limitata, il rischio è trascurabile o limitato

Valutazione : Accettabile

Modifiche indesiderate dei dati

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

Impatto limitato o significativo.

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

Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

Quali sono le fonti di rischio?

Fonti umane interne, fonti umane esterne, fonti non umane.

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

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dell'hardware, Sicurezza dei documenti cartacei, Controllo degli accessi fisici, Minimizzazione dei dati, Lotta contro il malware, Backup, Gestione del personale, Sicurezza dei canali informatici, Gestione dei terzi che accedono ai dati

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

Importante, limitato o importante.

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

Importante, limitato o importante.

Valutazione : Accettabile

Perdita di dati

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

Limitato o significativo.

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

Errore materiale, evento doloso o abuso di ufficio da parte di addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzate.

Quali sono le fonti di rischio?

Fonti umane interne, fonti umane esterne, fonti non umane.

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

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità, Lotta contro il malware, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Prevenzione delle fonti di rischio, Controllo degli accessi fisici, Gestione dei rischi, Gestione del personale, Gestione dei terzi che accedono ai dati

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

Importante, trascurabile o limitato

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

Limitata, trascurabile o limitato

Valutazione : Accettabile

Panoramica

Principi fondamentali

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

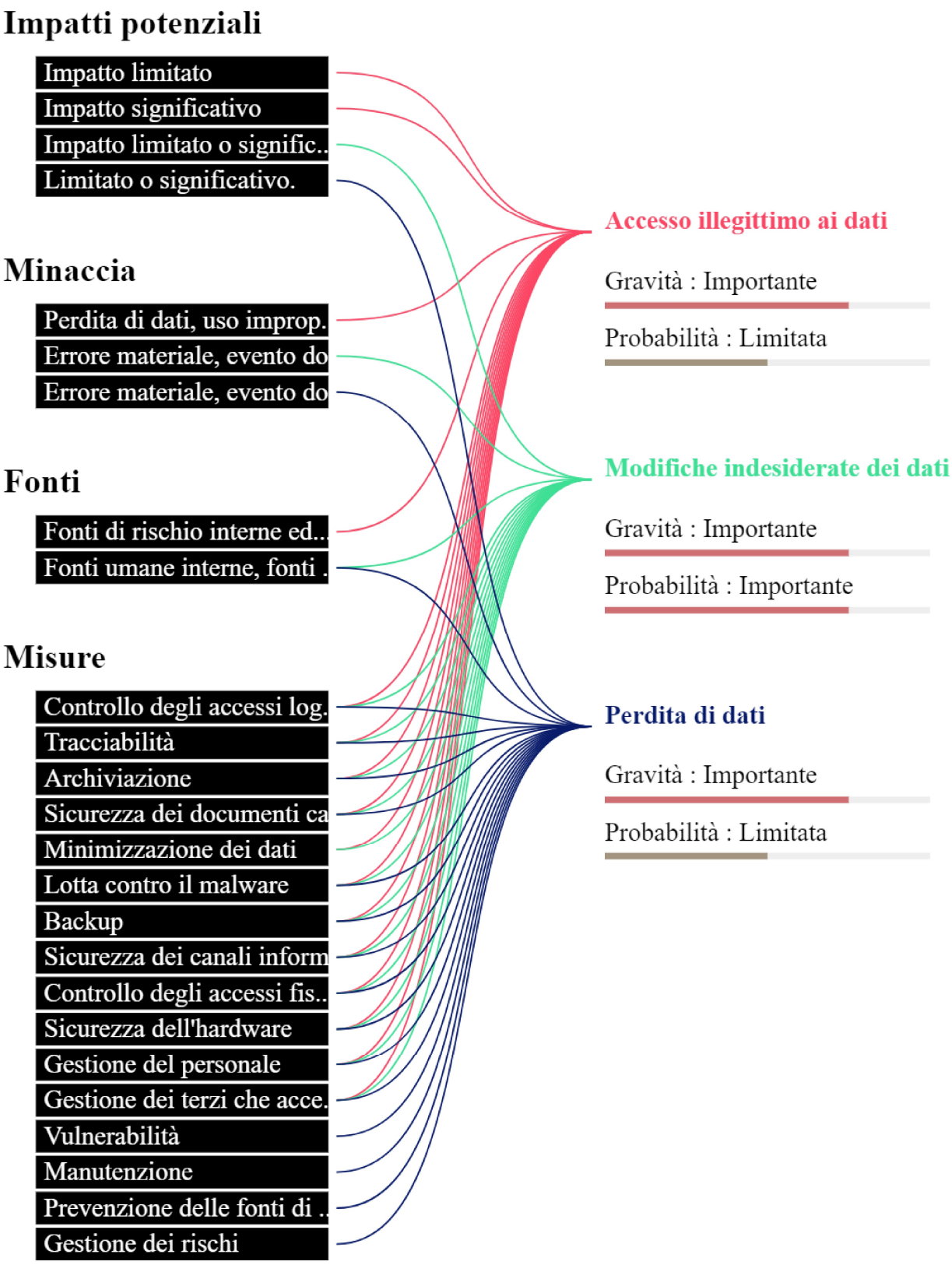
Misure esistenti o pianificate

- Anonimizzazione
- Controllo degli accessi logici
- Tracciabilità
- Archiviazione
- Sicurezza dei documenti cartacei
- Minimizzazione dei dati
- Vulnerabilità
- Lotta contro il malware
- Backup
- Manutenzione
- Sicurezza dei canali informatici
- Controllo degli accessi fisici
- Sicurezza dell'hardware
- Prevenzione delle fonti di rischio
- Politica di tutela della privacy
- Gestione dei rischi
- Gestione del personale
- Gestione dei terzi che accedono ai dati
- Specifiche misure di sicurezza

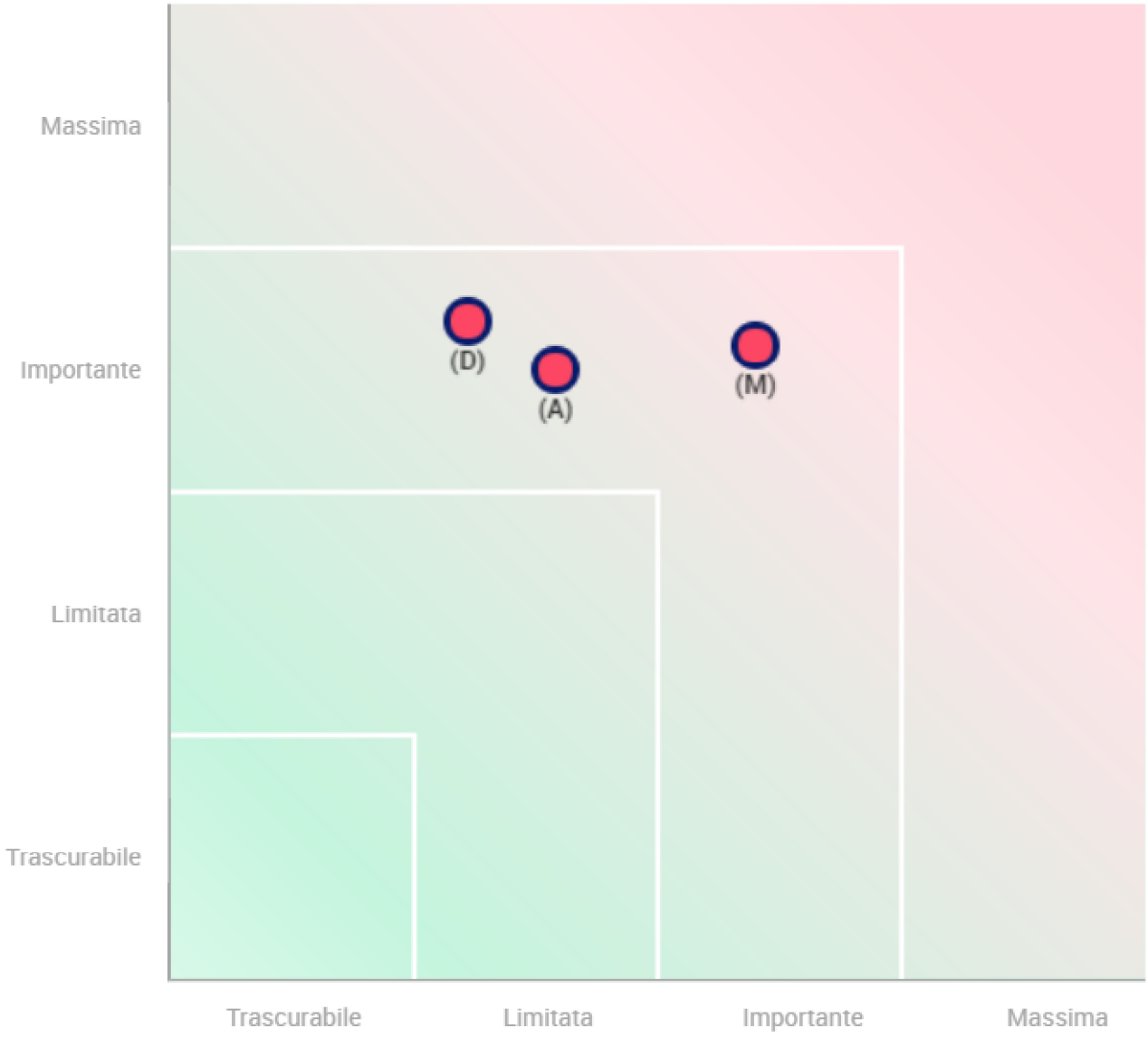
Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Misure Migliorabili
Misure Accettabili


Impatti potenziali
Impatto limitato
Impatto significativo
Impatto limitato o signific..
Limitato o significativo.
Minaccia
Perdita di dati, uso improp.
Errore materiale, evento do
Errore materiale, evento do
Fonti
Fonti di rischio interne ed..
Fonti umane interne, fonti .
Misure
Controllo degli accessi log.
Tracciabilità
Archiviazione
Sicurezza dei documenti ca
Minimizzazione dei dati
Lotta contro il malware
Backup
Sicurezza dei canali inform
Controllo degli accessi fis..
Sicurezza dell'hardware
Gestione del personale
Gestione dei terzi che acce.
Vulnerabilità
Manutenzione
Prevenzione delle fonti di ..
Gestione dei rischi
Accesso illegittimo ai dati
Gravità : Importante
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Importante
Probabilità : Importante
Perdita di dati
Gravità : Importante
Probabilità : Limitata

Gravità del rischio



Probabilità del rischio

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