DPIA PB - Preview

TO TRANSLATE - GENERAL INFORMATION

modifica pia

100%

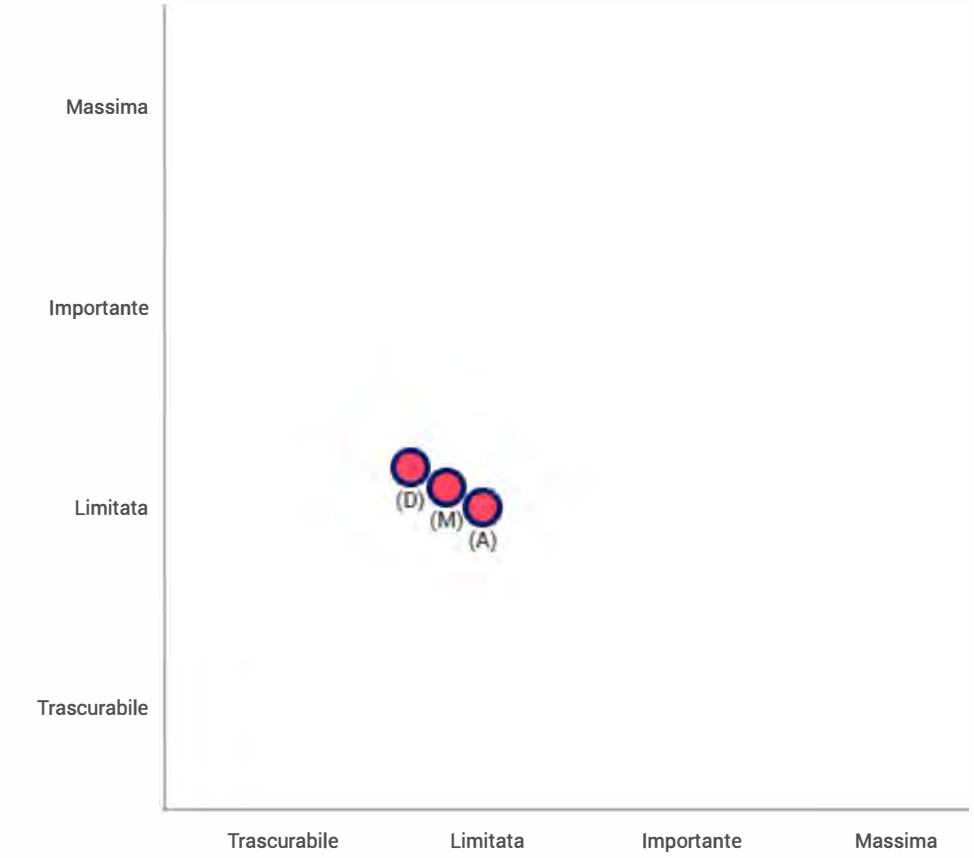
Anteprima

TO TRANSLATE - Editing :	Comune di Ponte Buggianese	**TO TRANSLATE - Status :**	Validata e firmata
TO TRANSLATE - Evaluation :	Riccardo Narducci		
TO TRANSLATE - Validation :	Renzo Giuntoli		

DPIA - Validation

Mappaggio dei rischi

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

11/04/25

DPIA - Validation

Piano d'azione

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
Tracciabilità
Archiviazione
Minimizzazione dei dati
Gestione postazioni
Manutenzione
Contratto con il responsabile del trattamento
Sicurezza dei canali informatici
Controllo degli accessi fisici
Protezione contro fonti di rischio non umane
Partizionamento

Rischi

Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

[redacted]

DPIA - VIDEOSORVEGLIANZA PM PONTE BUGGIANESE

Nome del DPO/RPD

Dott. Riccardo Narducci

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

policy e strumentazione compliant al GDPR

Richiesta del parere degli interessati

È stato chiesto il parere degli interessati.

Nomi degli interessati

Renzo Giuntoli

Posizione degli interessati

Il trattamento può essere implementato.

Pareri degli interessati

raccolte tutte le iinformazioni empiricamente e dcumentate tecnicamente tramite supporto DPO e Tecnici impianto videosorveglianza e ced comunale

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Trattamento di videosorveglianza per le seguenti finalità:
- tutela del patrimonio pubblico comunale;
- promozione ed attuazione della sicurezza integrata e della sicurezza urbana di cui agli artt. 4-5 del D.L. n. 14/2017, convertito con modificazioni dalla legge n. 48/2017. L'art. 6, c. 7 del D.L. 23 febbraio 2009 n. 11, convertito dalla legge n. 38/2009 stabilisce che per la tutela della sicurezza urbana i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici od aperti al pubblico;
- monitoraggio e controllo del traffico in tempo reale;
- lettura automatizzata delle targhe dei veicoli in circolazione per finalità amministrative connesse alla rilevazione, contestazione e sanzionamento delle violazioni in materia di circolazione stradale ed alla verifica dell'assolvimento degli obblighi previsti dal C.d.S. tra cui la revisione ed assicurazione obbligatoria dei veicoli;
- prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (D.Lgs. n. 51/2018). L'eventuale utilizzo del sistema di videosorveglianza per dette finalità, con sistematico accesso da parte di altre Forze di polizia o di sicurezza, dovrà essere disciplinato con appositi accordi secondo la vigente disciplina;
- prevenzione, accertamento e repressione degli illeciti derivanti dall'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose, nonché al rispetto della normativa concernente lo smaltimento dei rifiuti.

L'art. 2- sexies, c. 2, lett. l) del Codice privacy considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico nelle "attività di controllo ed ispettive".

Quali sono le responsabilità connesse al trattamento?

La responsabilità del titolare è connessa alla tipologia di trattamento che implica la sorveglianza sistematica su larga scala di aree del territorio comunale.
Il responsabile del servizio di Polizia locale è stato incaricato di specifici compiti e funzioni connessi al trattamento; lo stesso ha designato gli incaricati del trattamento. Le responsabilità del trattamento sono connesse al ruolo ricoperto.
E' individuato il responsabile del trattamento esterno nel manutentore esterno del sistema di videosorveglianza. Il sistema è previsto possa risultare aperto alle Forze di Polizia, determinandosi una contitolarità.

Ci sono standard applicabili al trattamento?

Il Garante per la protezione dei dati personali ha adottato il Provvedimento in materia di sorveglianza 8 aprile 2010.
Il Comitato europeo per la protezione dei dati ha adottato il 29 gennaio 2020 le Linee guida sui

Il Comitato europeo per la protezione dei dati ha adottato il 20 gennaio 2020 le Linee guida sui trattamenti dei dati personali attraverso dispositivi video.

Valutazione : Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Sono raccolte immagini delle aree indicate nell'allegata relazione tecnica. I dati personali che possono essere trattati sono costituiti dalle immagini delle persone fisiche ed i dati identificati degli autoveicoli (targhe) ripresi dalle telecamere che compongono il sistema.

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

Il trattamento è effettuato in base alle modalità tecniche in conformità alle disposizioni del regolamento comunale sulla videosorveglianza. Le immagini possono essere viste in tempo reale direttamente presso il comando della Polizia municipale da persone autorizzate (agenti di pubblica sicurezza).
Le immagini sono sovrascritte in modo automatico dopo sette giorni dalla loro rilevazione. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante il sistema è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione.
Le immagini riprese dalle telecamere vengono trasmesse attraverso un collegamento hyperlan 5 GHZ e si districa da una distribuzione dei dispositivi di rete (switch) posti nella sala di controllo nei locali della Polizia Municipale, e poi si districa verso il centrostella nella sala Ced dell'Ente per arrivare sui server virtualizzati e dispositivo Storage di rete dedicato con supporti magnetici e poi su dispositivo di back-up dedicato.
Le telecamere, come sopra Indicate, consentono, tecnicamente, riprese video a colori In condizioni di sufficiente illuminazione naturale o artificiale, o, in caso contrarlo in bianco/nero.
Tali caratteristiche tecniche consentono un significativo grado di precisione e di dettaglio della ripresa.
Nella Sede della Polizia Municipale questa sede le immagini saranno visualizzate su di un PC e Monitor dedicati a cui si accede solo tramite credenziali personali degli utenti autorizzati della Polizia Municipale e da lì si procede con ulteriore autenticazione per accesso alla versione client del software di consultazione delle immagini anche in Real-Time verso il Server Centrale virtualizzato.
Mentre le immagini fotografiche o video riprese dalle foto-trappole sono trasferite su di un software dedicato in dotazione alla sala di controllo; il trasferimento di dati dalla foto-trappola al portale informatico avviene manualmente senza collegamenti con altri sistemi o con altre reti pubbliche di telecomunicazioni, né attraverso l'accesso di altre periferiche ed è effettuato dal designato o dai preposti, muniti di credenziali di accesso (nome utente di dominio e password).
L'accesso alla sala di controllo è consentito solamente alla persona designata al trattamento dei dati, ai preposti nonché al personale: addetto alla manutenzione degli impianti, designato dal responsabile del trattamento, per la pulizia dei locali e delle forze dell'ordine.
Eventuali accessi di persone diverse da quelli innanzi indicate sono autorizzati per iscritto, dal designato del trattamento.
Essi vigilano sul puntuale rispetto delle istruzioni e sulla corretta applicazione delle disposizioni impartite dal titolare o dal designato del trattamento.
Il/I monitor degli impianti di videosorveglianza è collocato in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

Quali sono le risorse di supporto ai dati?

Il trattamento è effettuato mediante telecamere di rete dai soli agenti di polizia municipale con qualifica di agenti di pubblica sicurezza. I dati sono conservati in una partizione di memoria su un Server virtuale fisicamente salvato su un dispositivo di tipo S.A.N., come meglio precisato nell'allegato tecnico. È utilizzato software licenziato fornito dalla ditta Smau-Gfi srl, i cui operatori possono accedere al data base solo in caso di necessità tecnica, per manutenzione, senza possibilità di modificare le immagini.

Firewall funzionanti in cross-load, Switch di rete ridondati, Linee Dati principali e di back-up, server in cross load, antivirus dedicati. Storage SAN dedicato, nas per back-up dedicato, identity manager per controllo accessi, PC Client e WorkStation Analisi dati.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

La tutela del patrimonio comunale, della sicurezza stradale, della tutela ambientale e delle eventuali violazioni alle disposizioni che le regolano, sono compiti di interesse pubblico attribuiti al Comune.
A fini di sicurezza urbana i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici od aperti al pubblico ai sensi dell'art. 6, c.7, D.L. 23 febbraio 2009 n. 11, conv. in legge n.38/2009.
Il trattamento dei dati personali acquisiti mediante il sistema di videosorveglianza gestito dal Comune si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza ed all'identità personale.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento è lo svolgimento di compiti di interesse pubblico per le attività di controllo e prevenzione ai sensi dell'art. 6, lett. e), GDPR e dell'art.2-sexies, lett. l), Codice privacy, e per fini di prevenzione, indagine, accertamento e perseguimento di reati, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, ai sensi del D.Lgs. n. 51/2018.

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)?

Il trattamento dei dati attraverso il sistema di videosorveglianza comunale è proporzionale e legittimo rispetto alle finalità, tenuto conto degli interessati e del territorio. Non sono raccolti e/o estrapolati dati ai fini di un processo decisionale automatizzato, nè per profilazione nè per analisi predittive del comportamento degli interessati.
L'utilizzo del sistema di videosorveglianza comporta esclusivamente il trattamento dei dati personali rilevati mediante le riprese video e foto dei soggetti che, in relazione ai luoghi di installazione delle telecamere, transitano nell'area oggetto di sorveglianza; non sono rilevati audio e suoni.
Il posizionamento e le inquadrature del sistema di telecamere determina l'inquadramento esclusivamente di porzioni di aree pubbliche, escludendo, con apposite modalità, l'inquadratura di aree private, diversamente potendosi determinare una incisione dei diritti e delle libertà personali degli interessati.
L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite nelle sole aree predefinite, evitando, quando non indispensabile, immagini dettagliate, ingrandite o con particolari non rilevanti, e registrando le sole immagini indispensabili.
Il sistema è previsto già in origine che non raccolga i lineamenti dei volti e i dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi; ad es., per monitorare il traffico sono effettuate solo riprese generali che escludono la possibilità di ingrandire le immagini e rendere identificabili le persone o le targhe dei veicoli.
Le disposizioni recate dal regolamento comunale sulla videosorveglianza sono rivolte a limitare il trattamento di dati personali; il brandeggio delle telecamere è soggetto a limitazioni.
Le scelte inerenti la dislocazione delle telecamere e le modalità di ripresa sono effettuate in modo da limitare il trattamento rispetto alle finalità perseguite.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati personali sono costituiti da immagini riprese direttamente dalle telecamere installate. Ogni accesso ai dati archiviati è registrato mediante file di log. Agli incaricati è inibita ogni possibilità di modifica delle registrazioni mediante previsione specifica del software.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati registrati sono conservati per un periodo massimo di sette giorni successivi alla rllevazione, fatte salve speciali esigenze di ulteriore conservazione per finalità investigative, come previsto dalle disposizioni del regolamento comunale di videosorveglianza.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati tramite l'installazione di più cartelli con informativa sintetica di primo livello (segnale di avvertimento), collocati nelle immediate vicinanze delle telecamere, in modo ben visibile. Una informativa completa di secondo livello, nella quale è indicato anche il possibile utilizzo delle immagini da parte di altre Forze di Polizia, è disponibile presso il Comando della Polizia locale, sito in via Matteotti n. 76 - Ponte Buggianese, nonché sul sito web istituzionale dell'Ente.
Gli interessati sono resi informati circa le modalità e le aree soggette a videosorveglianza mediante la pubblicazione sul sito internet istituzionale di planimetrie ed altra documentazione relativa.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile.

Valutazione : Accettabile

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

È disponibile presso il Comando di Polizia ed è scaricabile dal sito web istituzionale dell'Ente apposita modulistica; sul sito sono pubblicati un estratto delle disposizioni normative inerenti i diritti degli interessati e slides del Garante della privacy di spiegazione di tali diritti e relative modalità di esercizio.

Valutazione : Accettabile

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

È disponibile presso il Comando di Polizia ed è scaricabile dal sito web istituzionale dell'Ente apposita modulistica; sul sito sono pubblicati un estratto delle disposizioni normative inerenti i diritti degli interessati e slides del Garante della privacy di spiegazione di tali diritti e relative modalità di esercizio.

Valutazione : Accettabile

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

È disponibile presso il Comando di Polizia ed è scaricabile dal sito web istituzionale dell'Ente apposita modulistica; sul sito sono pubblicati un estratto delle disposizioni normative inerenti i diritti degli interessati e slide del Garante della privacy di spiegazione di tali diritti e relative modalità di esercizio.

Valutazione : Accettabile

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

È stipulato un atto di natura contrattuale fra titolare e responsabile del trattamento, cioè la ditta esterna fornitrice del sistema e cura la manutenzione dello stesso, che vincola quest'ultimo a specifici istruzioni ed obblighi inerenti il trattamento allo stesso affidato.

Valutazione : Accettabile

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

In via ordinaria non sussiste trasferimento dei dati al di fuori della UE. In via ipotetica cioè è possibile solo in relazione a procedimenti giudiziari da parte delle competenti autorità, nei casi previsti dalla legge.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Controllo degli accessi logici

Le immagini raccolte sono accessibili soltanto agli agenti di PM con qualifica di agenti di pubblica sicurezza. E' possibile l'accesso da parte di altre Forze di Polizia in relazione a procedimenti giudiziari.
E' possibile l'accesso di incaricati della ditta fornitrice del server per interventi tecnici di manutenzione.
L'accesso è limitato ai predetti soggetti mediante username e password.

Valutazione : Accettabile

Tracciabilità

Ogni operazione compiuta sui sistemi è registrata nel log degli eventi.
Il log eventi ha una durata programmabile e conserva tutti gli eventi di sistema sia a livello Firewall che della Macchina Virtuale (come, ad esempio, gli accessi da parte degli utenti).
Gli accessi sono tracciati mediante file di log, con periodo di conservazione pari ad un massimo di 180 gg.

Valutazione : Accettabile

Archiviazione

È utilizzato il software di gestione licenziato per la registrazione delle immagini. L'archiviazione dei dati viene effettuato su un dispositivo S.A.N. MSA dedicato con due controller di memoria e 46 pool di dischi fisici configurati in RAID 5 e con Global Spare e Dischi SSD per caching dei dati.
Dal server virtuale per registrazione è impostata una retention di 7 (SETTE) giorni.
È previsto un back-up giornaliero dei dati di configurazione della macchina di tipo incrementale su

dispositivo NAS configurato in RAID 5 appositamente dedicato, ed un back- up completo a cadenza settimanale.
In entrambi i casi le retention più vecchie vengono automaticamente scartate dopo il periodo di 7 (SETTE) giorni come sopra indicato.

Valutazione : Accettabile

Minimizzazione dei dati

Il sistema è conformato in modo da non utilizzare dati relativi a persone identificabili quanto le finalità del trattamento possono essere realizzate impiegando solo dati anonimi, come, ad es., nel caso del monitoraggio del traffico.

Valutazione : Accettabile

Gestione postazioni

Postazione interna ad area allarmata degli uffici della Polizia Municipale.
Il PC, sito nell'ufficio della sala di controllo che necessita di apposita chiave per l'accesso, è utilizzabile solo dal designato o dai preposti muniti di credenziali di accesso personali.
Il server al momento non è munito di monitor e non necessita di accesso da parte del personale in loco.

Valutazione : Accettabile

Manutenzione

Esistenza di una politica di manutenzione fisica dei dispositivi a cura del responsabile esterno.

Valutazione : Accettabile

Contratto con il responsabile del trattamento

Manutenzione ordinaria e straordinaria dell'impianto con accesso anche da remoto sul sistema software.

Valutazione : Accettabile

Sicurezza dei canali informatici

Nel Data Center vi sono 2 dispositivi firewall che lavorano in crossload.
Il sistema di cctv è attestato su n. 2 VLAN separate logicamente dal resto delle VLAN, come da allegato tecnico.
Il server virtualizzato ed il PC hanno accesso bloccato alla rete esterna, è permesso il traffico solo verso i sistemi che forniscono manutenzione del software. I server virtuale dialoga anche con la rete ove risiedono le videocamere e la macchina preposta per il Back-UP.
I software e l'hardware sono aggiornati al bisogno durante l'attività di manutenzione compiuta dai Tecnici della videosorveglianza e Amministratore di sistema su mandato del Responsabile del trattamento dei dati.
I protocolli non necessari sono chiusi e bloccati dai dispositivi firewall e dalle policy di sicurezza che vengono aggiornate su bollettini dei Vendor dei software utilizzati.
Su server virtuale e PC è presente una licenza antivirus centralizzato. Un'ulteriore suite Antivirus licenziato è presente sui firewall in utilizzo.

Valutazione : Accettabile

Controllo degli accessi fisici

Esiste un controllo degli accessi fisici ai locali che ospitano il trattamento: zonizzazione con accesso

riservato, porte chiuse, allarmi anti intrusione presso gli uffici del Servizio di PM.

Valutazione : Accettabile

Protezione contro fonti di rischio non umane

Normali misure preventive, di rilevamento e di protezione per ridurre od evitare i rischi connessi a fonti non umane - sede della Protezione Civile.

Valutazione : Accettabile

Partizionamento

I dati sono conservati in partizione di memoria su server virtuale, come da allegato tecnico.

Valutazione : Accettabile

Rischi
Accesso illegittimo ai dati

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

Perdita di confidenzialità, Perdita di integrità, Perdita di disponibilità

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Uso apparecchiature tecnologiche, Soggetti coinvolti nel trattamento, Contatti con altre autorità, Accesso alle reti ed ai servizi di rete

Quali sono le fonti di rischio?

Persone interne ed esterne all'Ente operante in via accidentale od intenzionale, Attaccante esterno all'Ente, Comunicazione dei dati all'esterno dell'Ente

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Gestione postazioni, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane, Minimizzazione dei dati, Partizionamento

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

Limitata, Limitata. L'accesso illegittimo potrebbe determinare un impatto potenziale significativo per i diritti e le libertà delle persone fisiche, impatto che alla luce delle misure pianificate ed implementate può considerarsi accettabile.

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

Limitata, Limitata. Le misure pianificate ed implementate sono adeguate rispetto al rischio.

Valutazione : Accettabile

Rischi
Modifiche indesiderate dei dati

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

Perdita di integrità, Perdita di disponibilità

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

Uso apparecchiature tecnologiche, Soggetti coinvolti nel trattamento, Contatti con altre autorità, Accesso alle reti ed ai servizi di rete

Quali sono le fonti di rischio?

Persone interne od esterne all'Ente, operanti in via accidentale od intenzionale, Fonte non umana (eventi atmosferici, eventi naturali), Attaccante esterno

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

Controllo degli accessi logici, Tracciabilità, Sicurezza dei canali informatici, Protezione contro fonti di rischio non umane, Archiviazione, Gestione postazioni, Controllo degli accessi fisici, Contratto con il responsabile del trattamento, Minimizzazione dei dati, Partizionamento, Manutenzione

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

Limitata,

Limitata. Il rischio potenziale è limitato.

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

Limitata,

Limitata. Le misure applicate ed implementate sono adeguate rispetto al rischio.

Valutazione : Accettabile

Rischi

Perdita di dati

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

Perdita di integrità, Perdita di disponibilità

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

Uso apparecchiature tecnologiche, Soggetti coinvolti nel trattamento, Accesso alle reti ed ai servizi di rete, Contatti con altre autorità

Quali sono le fonti di rischio?

Persone interne ed esterne all'Ente operanti in via accidentale od intenzionale, Fonte non umana (eventi atmosferici, eventi naturali), Attaccante esterno

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

Archiviazione, Gestione postazioni, Manutenzione, Protezione contro fonti di rischio non umane, Sicurezza dei canali informatici, Controllo degli accessi fisici, Controllo degli accessi logici, Tracciabilità, Contratto con il responsabile del trattamento

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

Limitata,

Limitata. Il rischio attese le misure pianificate ed implementate è limitato.

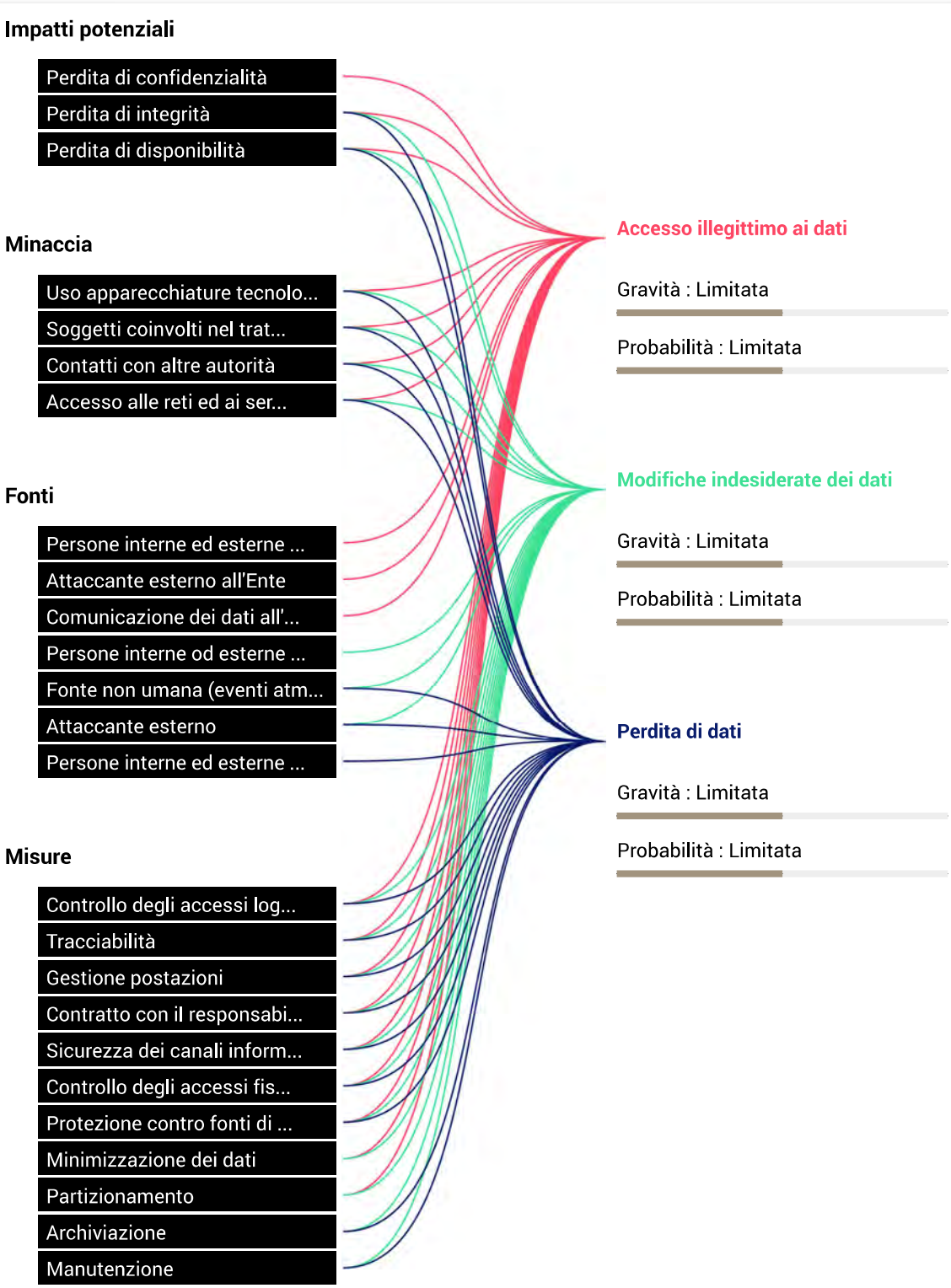
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

alle fonti di rischio e alle misure pianificate?

Limitata,

Limitata. Le misure pianificate ed implementate sono adeguate rispetto al rischio.

Valutazione : Accettabile

Rischi

Panoramica dei rischi