COMUNE
DI
MIRANDOLA
Città dal 1597

Valutazione d'impatto

Data Protection Impact Assessment (DPIA)

Titolare del trattamento
Comune di Mirandola

Responsabile del trattamento
Comune di Mirandola

Data approvazione

Sommario

1. Valutazione d'Impatto: fasi e realizzazione 3
2. FASE I: Definizione dell'operazione del trattamento e del suo contesto..... 4
3. FASE II: Comprensione e verifica della necessità di attuare una valutazione d'impatto 11
4. FASE III: Definizione di possibili minacce, valutazione della loro probabilità e valutazione del rischio 12
5. FASE IV: Conclusione della DPIA e definizione azioni conseguenti 21

1. Valutazione d'Impatto: fasi e realizzazione

La Valutazione d'impatto sarà condotta in base alle seguenti fasi:

Fase	A cosa serve	Come	Quando
Fase I Definizione dell'operazione di trattamento e del suo contesto	Serve a capire se nell'iniziativa sono presenti elementi minimi di rischio da approfondire con una valutazione di impatto ai fini GDPR	Tramite check list presente nella Fase I	Ogni volta che sia pianificata un'iniziativa o un progetto che preveda un possibile rischio nel trattamento dei dati personali. Da attivare fin dall'inizio della progettazione
Fase	A cosa serve	Come	Quando
Fase II Comprensione e verifica della necessità di attuare una valutazione dell'impatto	Con gli elementi raccolti in FASE I si è in grado di decidere se attivare o meno una valutazione di impatto	Attraverso l'analisi dei risultati di Fase I e con parere del DPO (se presente)	Al termine della FASE I e comunque prima dell'inizio del trattamento dei dati
Fase	A cosa serve	Come	Quando
Fase III Definizione di possibili minacce, valutazione della loro probabilità e valutazione del rischio	Questa fase serve ad effettuare la valutazione dell'impatto vera e propria	Tramite la check list e le tabelle di valutazione	Prima dell'inizio del trattamento dei dati
Fase	A cosa serve	Come	Quando
Fase IV Conclusione della DPIA e azioni conseguenti	Questa fase serve a valutare gli esiti della valutazione d'impatto e decidere le azioni conseguenti	Con il supporto del DPO (se presente)	Prima dell'inizio del trattamento dei dati

2. FASE I: Definizione dell'operazione del trattamento e del suo contesto

La FASE I ha come obiettivo l'individuazione delle peculiarità del trattamento oggetto di analisi e serve al Titolare del trattamento per identificare eventuali rischi da approfondire con una valutazione d'impatto privacy.
Al fine di una valutazione del rischio connessa al trattamento, è necessario descrivere il contesto e gli elementi caratterizzanti del trattamento stesso.

A tal fine vengono raccolte le seguenti informazioni:

- in cosa consiste l'attività di trattamento
- quali sono le tipologie di dati personali trattati
- quali sono le finalità del trattamento
- quali sono gli strumenti utilizzati per il trattamento dei dati personali
- dove avviene il trattamento dei dati personali
- quali sono le categorie di soggetti interessate
- chi sono i destinatari dei dati

Descrizione dell'ambito del trattamento

► **Descrizione breve del trattamento**

In questa DPIA verrà considerato il trattamento dei dati acquisiti dai seguenti gruppi di videocamere alcune delle quali sono già istallate e altre da installare in quanto facenti parte di un progetto di adeguamento e ampliamento dell'impianto:

1. telecamere Bullet fisse di videosorveglianza
2. telecamere Dome brandeggianti di videosorveglianza
3. telecamere di lettura targhe
4. videocamere riposizionabili c.d. "Fototrappole"
5. bodycam
6. eventuali telecamere riposizionabili che vengono prese a noleggio da Società esterne

Il trattamento in oggetto consiste nella registrazione dei flussi acquisiti dalle videocamere attualmente su 1 server e successivamente su 4 server (il server già esistente registrerà le immagini trasmesse dalle telecamere di lettura targhe e gli altri 3 server registreranno le immagini trasmesse dall'impianto di videosorveglianza) situati presso la sala server del Comune di Mirandola e nella loro consultazione a fronte di indagini di Polizia Giudiziaria, di incidenti stradali o del riscontro di danneggiamenti della proprietà pubblica. E' anche possibile da parte del Comandante di Polizia Locale, nominato Responsabile del trattamento dal Titolare, e dagli operatori dell'Ente da lui incaricati, la consultazione in tempo reale dei flussi video dalla sala di controllo della Polizia Locale. Il Responsabile e i suoi incaricarti possono effettuare la consultazione dei flussi tramite postazioni, a questo abilitate e dotate del necessario software.
Il Server attuale è dotato, così come quelli che verranno installati successivamente, di un sistema di backup dei dati, pertanto la ridondanza dei dati avverrà su un apparato Nas esterno, ubicato in una stanza diversa da quella dove saranno situati i Server.
Le telecamere c.d. "Fototrappole" registrano le immagini su una scheda di memoria interna. Le immagini vengono trasferite direttamente al software di gestione in forma criptata. Le immagini si cancellano automaticamente dopo 7 giorni se non devono essere conservate per un periodo più lungo. In questo ultimo caso vengono scaricate dal software.
Le telecamere bodycam vengono assegnate direttamente dal software di gestione e prelevate dall'operatore attraverso l'utilizzo del badge. Alla fine del servizio le immagini vengo scaricate automaticamente su PC e sono accessibili sono con l'utilizzo di credenziali personali. Le registrazioni sono attribuite all'operatore che ha indossato la telecamera ed effettuato le registrazioni stesse.
Le immagini registrate sono cancellate dopo 7 giorni, se non vi sono motivi, come indagini in corso, per prolungare il periodo di conservazione.
L'operatore non può in alcun modo cancellare e/o modificare le immagini.
La Polizia Locale del Comune di Mirandola inoltre, ha l'accesso attraverso proprie credenziali, alle immagini delle telecamere installate sui varchi veicolari dell'Unione dei Comuni Modenesi Area Nord per accordi presi

con l'Unione. Le immagini sono registrate su un server di proprietà dell'Unione dei Comuni.

► Base giuridica del trattamento

GDPR Regolamento UE 2016/679 del 27 aprile 2016, in particolare:
Art. 6, comma 1, lettera e):
il trattamento è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

► Destinatari dei dati

In caso di indagine o necessità di controllo a seguito del verificarsi di determinati eventi riscontrati durante il servizio: Autorità Giudiziaria - Procura della Repubblica, in caso di indagini dirette; Forze di Polizia competenti per territorio (Carabinieri, Polizia di Stato, Guardia di Finanza) in caso di indagini indirette/delegate.

► Categorie di interessati coinvolti nel trattamento

Cittadini e/o comunque tutti i soggetti che vengono ripresi

► Principali fornitori del servizio

Società installatrice degli apparati e incaricata del servizio di manutenzione e assistenza:

- *F.G.S. Impianti s.r.l.* avente sede in Via Cremasca n. 90 – 24052 Azzano San Paolo (BG) – C.F. e P.IVA 01557310164;

Riferimenti tecnici hardware attualmente esistenti:

- Telecamere Mini Dome da 1MPx;
- Telecamere Dome da 2MPx;
- Telecamere Dome da 3MPx;
- Telecamere Dome da 4MPx;
- Telecamere Dome da 5MPx;
- Telecamere Bullet da 2 MPx;
- Telecamere Bullet da 3MPx;
- Telecamere Bullet da 4MPx;
- Telecamere Bullet da 5MPx
- Telecamere Bullet da 8MPx.
- Bodycam Reveal Modello 3
- Bodycam Reveal Modello 7
- Fototrappole E-Killer Flex 2.0

Riferimenti tecnici hardware che verranno installati;

- Telecamere Bullet da 4MPx;
- Telecamere Bullet da 6MPx;

- Telecamere Lettura targhe MOD.TS-5MPX-OCR-G o equivalente

► Risorse informatiche di supporto ai dati

I flussi acquisiti dalle videocamere sono registrati in modalità cifrata sui server dedicati situati presso la sala server del Comune di Mirandola. Il Responsabile e i suoi incaricarti possono effettuare la consultazione dei flussi tramite computer a questo abilitati e dotati del necessario software, tramite le rispettive utenze.
A seguire i dettagli tecnici dell'infrastruttura hardware e software:

- 1 Server di gestione e storage Dell EMC mod.R74XD da 40 TB esistente per il sistema di lettura targhe;
- 3 Server di gestione e storage mod. SR550-DA-24TB o equivalente per il sistema di videosorveglianza
- Switch Managed HP mod. Procurve (esistente)
- Switch Industriale mod.IGS-10020HPT o equivalente (implementazione impianto)
- Switch Industriale mod.IGS-1204MT o equivalente (implementazione impianto)
- Switch Industriale mod.IGS-5225-8P4S o equivalente (implementazione impianto)
- Switch Managed mod. TX2020R-P o equivalente (implementazione impianto)
- Monitor LCD da 27"
- Monitor LCD da 54"

► Area geografica di riferimento

Comune di Mirandola

Standard applicabili al trattamento

Nessuno

► Tipologia di dati trattati

Dati personali:

Immagini personali derivanti dalle inquadrature e/o dalle registrazioni che costituiscono identità fisica ex art. 4, comma 1, punto 1) del GDPR;

Categorie particolari:
☐ origine razziale o etnica
☐ opinioni politiche
☐ convinzioni religiose o filosofiche
☐ appartenenza sindacale
☐ dati genetici
☐ dati biometrici
☐ dati relativi alla salute o alla vita sessuale
☐ dati relativi all'orientamento sessuale
☐ dati giudiziari (condizione di reato, imputato, ecc.)
Nessuna

Dati giudiziari:
NO

► Tali dati vengono raccolti:
☐ direttamente presso l'interessato
☐ presso altre fonti, come:
☐ acquisto di data base
☐ dati pubblici
☐ dati raccolti sul web
☒ altro: inquadrature e registrazioni dalle videocamere

Analisi del trattamento dei dati

► Il trattamento prevede attività di profilazione o scoring (attribuzione di un punteggio) che possano, ad esempio, impattare sulla situazione economica, sulla salute, sugli interessi personali, sul comportamento, sull'ubicazione, sugli spostamenti, sulle abitudini di consumo, sul rendimento professionale, ecc. delle persone?
☐ Attività di profilazione
☐ Attività di scoring
☒ Nessuna delle precedenti

► Il trattamento prevede decisioni automatizzate che possano produrre effetti giuridici per i destinatari (ad es. esclusione da un contratto, da determinati benefici, ecc.) senza l'intervento di decisione umana?
☒ No
☐ Si

► Il trattamento prevede attività di monitoraggio sistematico o videosorveglianza?
☐ No
☒ Si:
☒ Videosorveglianza
☐ Rilevazione satellitare
☐ Altro

► Il trattamento prevede trattamenti su larga scala?
☐ No
☒ Si, nella fattispecie si tratta di
☐ numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento
☐ volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento

☐ durata, o persistenza, dell'attività di trattamento

☒ ambito geografico dell'attività di trattamento →Persone e veicoli transitanti nelle aree soggette a videosorveglianza

► Il trattamento prevede l'attività su dati relativi a interessati potenzialmente vulnerabili?

☒No

☐Si, nella fattispecie di tratta di:

- ☐disabili, incapaci
- ☐minori
- ☐anziani
- ☐persone con disagio
- ☐Altro

► Il trattamento prevede l'utilizzo di nuove tecnologie o soluzioni organizzative innovative?

☒ No

☐Si

► Il trattamento prevede il trattamento di dati genetici o biometrici?

Dati genetici: dati idonei a identificare patologie genetiche, malattie ereditarie, fattori di rischio genetico;

Dati biometrici: dati idonei a riconoscere iride o retina, impronte digitali, rilevazione facciale, rilevazione di andatura, movimento labbra, ecc.

☒No

☐ Si, nella fattispecie di tratta di:

- ☐dati genetici
- ☐dati biometrici

► Il trattamento prevede attività di geo localizzazione o geo referenziazione?

☒ No

☐Si

► Il trattamento prevede elaborazioni di dati finanziari relativi all'interessato?

☒ No

☐Si, nella fattispecie di tratta di:

- ☐

Responsabilità per l'utilizzo dei dati

► Chi è il titolare dei dati acquisiti nel progetto?

Il Comune di Mirandola

► Quali sono le figure interne del Titolare deputate al trattamento dei dati? Il Responsabile del trattamento, cioè il Comandante del Corpo di Polizia Locale e i suoi incaricati

► I dati possono essere condivisi/trattati da soggetti terzi? E per quali finalità?
☐ No
☒ Si, nella fattispecie di tratta di:
AUTORITA' GIUDIZIARIA E FORZE DI POLIZIA: per finalità di indagine e di polizia giudiziaria. I trattamenti hanno ad oggetto tutte le immagini acquisite per la suindicata finalità. Il Commissariato di Polizia di Mirandola ha accesso diretto alle immagini di videosorveglianza attraverso l'attribuzione di proprie credenziali.
SOCIETA' CHE SI OCCUPA DELLA MANUTENZIONE DELLE TELECAMERE: per finalità di manutenzione. I trattamenti hanno ad oggetto tutte le immagini visionate per la suindicata finalità
SOCIETA' CHE SI OCCUPA DELL'ASSISTENZA PER IL SOFTWARE: per interventi di assistenza. I trattamenti hanno ad oggetto tutte le immagini visionate per la suindicata finalità

► Sono stati predisposti i contratti di nomina a responsabili esterni con tutte le clausole previste dal GDPR?
Si

► I dati potranno essere trasferiti al di fuori dell'Unione Europea?
☒ No
☐ Si, nella fattispecie nei seguenti Paesi:

► I dati potranno essere condivisi con organizzazioni situate al di fuori dell'Unione Europea?
☒ No
☐ Si, nella fattispecie di tratta delle seguenti organizzazioni:

Finalità e modalità del trattamento

Tutela della sicurezza urbana, controllo del traffico, eventuali indagini di polizia giudiziaria e attività di tipo sanzionatorio in caso di abbandono illegittimo dei rifiuti (telecamere fototrappole).
In base a quanto previsto dal d.lgs. 150/2022 potranno essere effettuate su indicazioni della Procura, registrazioni dei soggetti ascoltati per l'assunzione di sommarie informazioni (con utilizzo di bodycam), finalizzate alla successiva trasmissione delle registrazioni agli organi preposti.

► Come si prevede che i dati siano conservati?
I dati, consistenti in fotogrammi e filmati video, saranno conservati per 7 giorni sui server sopra indicati e duplicati (back up) su un apparato NAS esterno ubicato in luogo differente rispetto ai locali ove sono siti i server. Qualora per le finalità sopra descritte risultasse necessario al Responsabile della videosorveglianza e/o a soggetti da lui incaricati acquisire copia in locale (nella proprie postazioni) di fotogrammi e/o filmati video, questi saranno conservati fino a quando non sia conclusa l'indagine di polizia giudiziaria. Le immagini riprese dalle telecamere c.d. Fototrappole sono registrate su una scheda memoria presente sulle telecamere stesse e vengono scaricate direttamente tramite trasmissione con scheda gsm sul pc dell'operatore; quelle riprese dalle bodycam sono registrate su una scheda memoria presente sulle telecamere stesse e vengono scaricate sul pc dell'operatore.

► I dati saranno aggiornati?
I dati non saranno aggiornati, ma semplicemente "conservati".

► Allo stato delle informazioni disponibili per quanto tempo si prevede di conservare i dati?
Per sette giorni, salvo che non emergano esigenze investigative e giudiziarie che richiedano un tempo di conservazione più lungo.

Diritti degli interessati

► È prevista la predisposizione di un'apposita informativa agli interessati e l'acquisizione del consenso degli stessi al trattamento dei dati?
☐ No, né informativa né consenso in quanto

☐ Si, informativa e consenso
L'informativa è resa all'interessato tramite:
☐ documento consegnato all'interessato
☐ altro
Il consenso è richiesto tramite

☒ Si, solo informativa
L'informativa è resa all'interessato tramite:
☐ documento consegnato all'interessato
☒ cartello contenente informativa breve presso → i luoghi presso i quali sono collocate le videocamere
☒ altro – Informativa pubblicata sul sito istituzionale

La richiesta di consenso NON è dovuta in quanto:
☐ il trattamento avviene in base ad un obbligo di legge
☒ i dati sono necessari per la tutela della sicurezza urbana, compito istituzionalmente affidato al Comune.

► Il progetto prevede il trattamento di dati personali per i quali il consenso agli interessati sia stato richiesto da terze parti?
☒ No

► E' prevista la redazione di un modello per l'esercizio dei diritti degli interessati?
☐ No
☒ Si
Come fanno gli interessati ad esercitare i loro diritti di:
- accesso: facendone richiesta al titolare/responsabile del trattamento
- rettifica: non applicabile
- integrazione: non applicabile
- cancellazione (oblio): è automatica
- portabilità: non applicabile
- opposizione: non applicabile
- limitazione: non applicabile
- reclamo all'Autorità: tramite esposto al Garante

Misure tecniche, fisiche ed organizzative per la sicurezza dei dati personali esistenti o pianificate

Visto l'art. 35, paragrafo 7, lettera c, del GDPR si è provveduto ad attuare le seguenti misure di sicurezza. Queste dovranno essere implementate con misure idonee, se necessario, secondo le disposizioni del Garante e la normativa un ambito di privacy ed in ottemperanza ai principi di responsabilizzazione ed accountability, secondo i quali il titolare del trattamento è tenuto all'adozione di ogni misura di sicurezza ritenuta idonea e necessaria a tutelare i diritti e le libertà dei soggetti interessati.

Misure organizzative:
-approvazione del Regolamento sulla Videosorveglianza;
-valutazione d'impatto dei trattamenti;
-registro dei trattamenti sulla videosorveglianza;
-istruzioni interne ai soggetti autorizzati al trattamento;
-nomina del responsabile;
-nomina del DPO;
-assegnazione degli incarichi;
-formazione degli incaricati al trattamento dei dati;
-predisposizione del registro delle richieste di estrazione delle registrazioni delle immagini da parte delle Forze di pubblica sicurezza (Carabinieri, Polizia di Stato etc.);
-sono state predisposte le disposizioni operative per l'utilizzo di Fototrappole e bodycam:
-controllo sull'operato degli addetti alla manutenzione dei sistemi di videosorveglianza;
-nomina a responsabili esterni degli addetti alla manutenzione dei sistemi di videosorveglianza;
-predisposizione informativa breve (cartellonistica) ed estesa (sito web Comune);
-nomina di un responsabile per la gestione delle chiavi della sala server;
-registrazione dei visitatori;
-Selezione attenta del personale ausiliario, ad es. addetti alle pulizie, guardie di sicurezza;
-limitazione del salvataggio in locale della documentazione che può essere effettuato solo dal Responsabile (Comandante Polia Locale) e dei soggetti dallo stesso incaricati;
-sottoscritto accordo di contitolarità con la Polizia del Commissariato di Mirandola che ha accesso diretto alle immagini di videosorveglianza;
-nel caso di acquisizione a noleggio di telecamere riposizionabili, verrà acquisita preventivamente la DPIA predisposta dalla società proprietaria delle telecamere

Misure fisiche:
-ricovero degli apparati in archivio con chiave;
Serrature di sicurezza;
-vigilanza della sede (Comune e Comando Polizia Locale), presenziamento diurno;
-attivazione dei sistemi di allarme antintrusione in assenza di presenziamento e in orari notturni/festivi;
Sistema per autorizzazioni di accesso per dipendenti e terze parti;
-Videosorveglianza degli ingressi;
-collocazione stazione di monitoraggio in ambiente vietato al pubblico;
-impianto anti-incendio;
-controllo degli accessi ai locali;
-esistenza di un gruppo di continuità in grado di alimentare il server in caso di interruzioni di corrente.

Misure tecniche e logiche:
identificazione del personale incaricato;

autenticazione degli accessi (PW di autorizzazione a più livelli);
registrazione degli accessi a dati e programmi (LO Creazione e utilizzo di profili utente a livello personale);
password con lunghezza minima, intervallo per la modifica delle password, minimo;
autenticazione con ID utente personale e password;
conservazione dei LOG per almeno 6 mesi;
criptazione delle trasmissioni;
controllo accessi logici;
sistemi di Protezione della Rete;
cambio forzato delle password con frequenza periodica trimestrale;
configurazione delle password per soddisfare il requisito di password sicura;
Utilizzo di un software antivirus ;
Utilizzo di un firewall software ;
Utilizzo di un firewall hardware;
attivazione del sistema di sospensione dei PC, screensaver;
Criptazione degli archivi di backup;
Blocco schermo automatico;
cifratura dei dati memorizzati su server e sui pc sui quali vengono scaricate le immagini di Fototrappole e Bodycam;
residenza temporanea dei dati su server e cancellazione automatica dopo 7 giorni mediante sovrascrittura;
backup dei dati su un apparato Nas esterno, ubicato in luogo differente rispetto ai locali ove è sito il server.

3. FASE II: Comprensione e verifica della necessità di attuare una valutazione d'impatto

► Alla luce delle informazioni fornite nella Fase I è necessario procedere con una valutazione di impatto sulla protezione dei dati personali?

☒ SI si passa alla FASE III

4. FASE III: Definizione di possibili minacce, valutazione della loro probabilità e valutazione del rischio

La valutazione dei rischi riflette un giudizio che nel tempo potrebbe cambiare in ragione dell'evoluzione del quadro normativo e della struttura organizzativa. Per questo l'organizzazione verifica con frequenza annuale il sistema di classificazione, di identificazione e mappatura delle aree a rischio, al fine di garantire una mappatura delle aree sensibili costantemente aggiornata. Il modello scelto per quantificare i rischi è quello della determinazione dell'esposizione al rischio:

Esposizione = probabilità x danno (impatto)

La valutazione del rischio è data dalla combinazione di due coefficienti:

- **probabilità** di accadimento della minaccia rilevata (la probabilità è legata anche all'esistenza o meno di strumenti di controllo/regole atti a prevenire il verificarsi della minaccia rilevata);
- **danno (impatto)** inteso come possibile effetto sulla dignità e libertà degli interessati oppure danni materiali allo stesso derivanti dal verificarsi dell'evento considerato a rischio.

Probabilità	Alta	4	4	8	12	16
	Media	3	3	6	9	12
	Bassa	2	2	4	6	8
	Improbabile	1	1	2	3	4
			1	2	3	4
			Trascurabile	Basso	Medio	Alto
			Danno			

Alto -> Intervento urgente

Medio -> Pianificare intervento entro l'anno

Basso-da monitorare

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

Il Titolare del trattamento in questa fase valuta l'impatto sui diritti e sulle libertà fondamentali delle persone fisiche derivanti dalla possibile perdita di sicurezza dei dati personali. Vengono considerati quattro livelli di Impatto (Basso, Medio, Alto, Molto Alto) come mostrato nella tabella seguente:

Livello di impatto	Descrizione
BASSO	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
MEDIO	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi del Titolare, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
ALTO	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTO	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Probabilità: Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Stimare il valore in base ai valori della seguente tabella:

Probabilità	Livello	Criterio probabilistico (probabilità di accadimento stimata nell'anno)
4	Quasi certo	Probabilità > 50%
3	Probabile	20% < Probabilità < 50%
2	Moderata	5% < Probabilità < 20%
1	Raro/Improbabile	Probabilità < 5%

Impatto stimato: 3 (Medio)
Probabilità stimata: 1 (Raro/Improbabile)=
Da cui: RISCHIO STIMATO 3x1=3 (MEDIO)

VALUTAZIONE DEL RISCHIO

La tabella indica la presenza o meno del rischio menzionato e fornisce una valutazione riguardante le probabilità di accadimento dell'evento lesivo e delle conseguenze (impatto) che l'evento può avere sui dati trattati.

Grado di Valutazione di Impatto e Rischio Residuo
Viene effettuata una valutazione per ogni classificazione di rischio, così da ottenere diversi livelli di impatto per ogni tipologia di rischio.
E' necessario riflettere sull'impatto che un trattamento non autorizzato, si riferisca esso alla divulgazione, alterazione, distruzione o perdita dei dati potrebbe avere sull'individuo, al fine di esprimere la valutazione.
Il più alto dei livelli stimati sarà considerato come il risultato finale relativo al trattamento complessivo dei dati.

Rischio residuo basso: valore stimato fino a 3
Rischio residuo medio: valore stimato da 3 a 8
Rischio residuo alto: valore stimato oltre 8

CLASSIFICAZIONE RISCHI

Rischi di distruzione o perdita dei dati
Rischi fisici
Per il Comune i rischi di distruzione o perdita dei dati sono da considerarsi genericamente riconducibili alle cause sotto elencate:
1. Incendio (per cause naturali, per comportamento colposo o doloso). Nell'ambito relativo alla classificazione del rischio incendio occorre comunque tenere presente quanto precisato, anche riguardo alle misure adottate nella valutazione dei rischi in ambito di sicurezza (626/94)
2. Allagamenti (per cause naturali, per comportamento colposo o doloso);
3. Scasso;
4. Perdita accidentale;
5. Sottrazione, furto di p.c.;

Rischi informatici
1. Caduta di energia elettrica;
2. Cancellazione fortuita di dati;
3. Accessi non consentiti;

4. Virus informatici;

Rischio stimato IXP
Impatto stimato 3 (Medio)
Probabilità stimata 1 (Raro/Improbabile)
RISCHIO STIMATO 3X1 =3 (Basso)

Rischi connessi all'integrità dei dati
Per il Comune i rischi connessi all'integrità dei dati sono da considerarsi genericamente riconducibili alle cause sotto elencate:
Rischi fisici
Manomissione dolosa dai dati-immagini (da parte di terzi o personale dipendente);
Alterazione dei dati colposa o errore umano (personale dip.);
Rischi informatici
Infezioni di virus
Errori nel software utilizzato
Attacchi informatici

Rischio stimato IXP
Impatti stimato 2 (Basso)
Probabilità stimata 1 (Raro/Improbabile)
RISCHIO STIMATO 2X1 =2 (Basso)

Rischi di accesso non autorizzato
Per il Comune i rischi di accesso non autorizzato sono da considerarsi genericamente riconducibili alle cause sotto elencate:
Rischi fisici
1. Intrusione di persone non autorizzate nei locali della sala di Controllo e nella sala server: luoghi in cui vengono visionati e conservati i dati;
2. Negligenza da parte del Titolare o del personale dipendente nel lasciare i dati incustoditi (porta sala operativa aperta, copia registrazioni immagini abbandonata sopra la scrivania, durante e dopo l'orario di lavoro) e non protetti (senza aver provveduto a chiudere le registrazioni dei dati o a riporre la chiave in un luogo sicuro);
3. Impossibilità da parte del Titolare o del personale dipendente di custodire i dati in luoghi adeguatamente protetti e sicuri in quanto gli archivi non sono muniti di chiavi o hanno la chiusura difettosa;
4 . Non osservanza (per motivi operativi) della necessaria segretezza nell'uso delle credenziali di accesso;
5. Mancata chiusura del posto di lavoro in caso di allontanamento, anche momentaneo, dell'operatore;

6. Controlli inadeguati sul personale esterno adibito all'assistenza tecnica;

Rischi informatici

1. Intrusione durante la trasmissione di dati;
2. Mancata disabilitazione dell'operatore del livello e dei profili di cui era in possesso prima dell'ultimo trasferimento;
3. Attacchi informatici e vulnerabilità del sistema

Rischio stimato IXP

Impatti stimato 3 (Medio)

Probabilità stimata 1 (Raro/Improbabile)

RISCHIO STIMATO 3X1 =3 (Basso)

Rischi di trattamento non consentito o non conforme alle finalità della raccolta

Per il Comune i rischi di trattamento non autorizzato o non conforme sono da considerarsi genericamente riconducibili alle cause sotto elencate:

Rischi fisici

1 Mancanza delle istruzioni impartite agli incaricati

2. Mancato recepimento delle disposizioni impartite agli incaricati e relative al trattamento dei dati;
3. Non completezza dell'informativa da fornire ai soggetti interessati;
4. Diffusione volontaria o colposa di dati a soggetti non legittimamente coinvolti nel trattamento;
5. Accesso e trattamento dei dati da parte di persone non autorizzate per difetto di controllo

6. Difetto di congruità delle credenziali di accesso
7. Mancata verifica e/o controllo nel caso di accessi della Società di manutenzione

Rischi informatici

1 Errori/vulnerabilità del software;

2Erroneo funzionamento delle credenziali di accesso.

Rischio stimato IXP

Impatti stimato 3 (Medio)

Probabilità stimata 1 (Raro/Improbabile)

RISCHIO STIMATO 3X1 =3 (Basso)

Rischi connessi alla trasmissione dei dati

Per il Comune i rischi connessi alla trasmissione dei dati sono da considerarsi genericamente riconducibili alle cause sotto elencate:

Rischi fisici

1. Caduta linea di trasmissione dati;
2. Danneggiamento - per guasto tecnico, manomissione dolosa, mancanza di energia elettrica di alimentazione - di dispositivi di interconnessione (modem, router, firewall)

Rischi informatici;

1. Intrusione di virus informatici atti a distruggere e/o manomettere i dati personali;
2. Intrusione da parte di soggetti esterni nella rete di trasmissione;

Rischio stimato IXP
Impatti stimato 3 (Medio)
Probabilità stimata 1 (Raro/Improbabile)
RISCHIO STIMATO 3X1 =3 (Basso)

Rischi connessi al reimpiego di supporti di memorizzazione
Per il Comune i rischi connessi al reimpiego di supporti mobili di memorizzazione sono da considerarsi genericamente riconducibili alle cause sotto elencate:
Rischi fisici

1. Accesso ai dati da parte di persone non autorizzate per mancata o incompleta cancellazione;
2. Trattamento non consentito o non conforme alle finalità della raccolta per mancata o incompleta cancellazione;
3. Duplicazione non consentita volontaria e/o colposa dei dati

Rischi informatici

1. Non sicurezza e vulnerabilità dei supporti mobili di memorizzazione
2. Attacchi informatici esterni

Rischio stimato IXP
Impatti stimato 3 (Basso)
Probabilità stimata 1 (Raro/Improbabile)
RISCHIO STIMATO 3X1 =3 (Basso)

Rischi connessi alla conservazione dei dati e della documentazione relativa al trattamento e alla riproduzione dei dati
Per il Comune i rischi connessi alla conservazione dei dati sono da considerarsi genericamente riconducibili alle cause sotto elencate:
Rischi fisici

1. Distruzione o perdita per incendio, alluvione, furto;

Rischi informatici

1. 1. Distruzione o /cancellazione dei dati per virus, attacchi esterni, malfunzionamenti e problematiche collegate alla gestione informatica e alla conservazione

dei dati stessi:

Rischio stimato IXP
Impatti stimato 3 (Medio)
Probabilità stimata 1 (Raro/Improbabile)
RISCHIO STIMATO 3X1 =3 (Basso)

RISULTATO FINALE RISCHIO RESIDUO:RISCHIO BASSO

Misure di mitigazione e azioni di miglioramento

- Rischio relativo ai tempi di recupero dei dati: la ridondanza dei dati è assicurata da un sistema di backup, ma deve essere valutata la possibilità di predisporre una procedura di disaster recovery per garantire la disponibilità dei dati in tempi brevi.
- Rischio relativo alla sicurezza della sala server: valutare lo stato dell'arte della sale server

Monitoraggio della temperatura e dell'umidità nella sala server
Sistema di allarme, allarme antincendio e fumo per sala server
Estintori nelle sale server
Regolamento chiave sala server

- Rischio relativo all'effettiva ridondanza dei dati: è auspicabile attivare un sistema di notifica dei backup anche in caso di esito positivo
  Archiviazione del backup in un luogo sicuro
- Rischio relativo alla sicurezza dei dati e ad accessi non consentiti: Deve essere predisposto un registro fisico degli accessi alle immagini.
- Rischio relativo all'accesso da parte della Società incaricata della manutenzione (responsabile esterno)
  Nel caso di interventi da remoto da parte della Società di manutenzione, l'intervento deve avvenire con modalità presidiata da parte del personale dell'Ente.
- Bodycam: rischio relativo alla mancata crittografia dei dati per l'arco temporale nel quale le immagini vengono registrate nella memoria della bodycam prima di essere riversate sui pc.

Al riguardo devono essere fornite specifiche istruzioni ai soggetti incaricati, affinchè il riversamento avvenga immediatamente al termine dell'utilizzo delle bodycam.
I tempi del riversamento devono essere esattamente definiti nel regolamento di utilizzo delle bodycam (disposizioni operativi e/o disciplinare tecnico).
Deve inoltre essere tenuto un registro fisico attestante il riversamento delle immagini contenente indicazioni circa data e orario delle operazioni di riversamento e deve essere prevista una verifica dello svolgimento di tale attività e della conseguente cancellazione delle immagini dall'apparato di registrazione interno alla bodycam prima della consegna della stessa per un nuovo servizio.

- Bodycam: rischio trattamenti non consentiti

Le disposizioni operative e/o il disciplinare tecnico devono contenere precise e dettagliate indicazioni riguardo alle situazioni, alle circostanze ed ai presupposti

per l'azionamento delle telecamere da parte dell'operatore.

5. FASE IV: Conclusione della DPIA

Sull'analisi in oggetto si è in attesa di parere del DPO

Valutazione finale

Alla luce delle informazioni raccolte e dei risultati ottenuti attraverso la presente valutazione d'impatto, si ritiene che:

È possibile procedere con l'implementazione del progetto e l'avvio del trattamento senza ulteriori misure tecniche e organizzative.

Firmato digitalmente
ALBERTO GRECO
Data: 12/07/2023 16