

Valutazione d'impatto

Data Protection Impact Assessment (DPIA)

Titolare del trattamento Comune di Monteleone d'Orvieto

Data approvazione
25 settembre 2024

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 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 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 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

Riferimenti normativi

- Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016
- Direttiva UE 2016/680 del Parlamento Europeo e decreto Legislativo n° 51 del 2018
- Linee Guida n. 3/2019 dell'European Data Protection Board (EDPB)
- Provvedimento generale del Garante in tema di videosorveglianza dell'8 aprile 2010

Descrizione dell'ambito del trattamento

► Descrizione breve del trattamento

In questa DPIA verrà considerato il trattamento dei dati acquisiti dai seguenti gruppi di videocamere:

telecamere fisse di lettura targhe e videosorveglianza urbana.

Il trattamento in oggetto consiste nella registrazione dei flussi acquisiti dalle videocamere su server situati presso la sala server del Comune di Monteleone d'Orvieto finalizzati a:

- a. prevenire e reprimere atti delittuosi, attività illecite anche di tipo amministrativo 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 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 d.lgs. 267/2000;
- b. acquisire automaticamente le liste aggiornate dei veicoli rubati, non assicurati o non revisionati;
- c. monitorare i flussi di traffico.

E' anche possibile da parte del Comandante della Polizia Locale, nominato Responsabile dell'impianto in qualità di Persona Autorizzata al trattamento sotto la diretta autorità del Titolare (art. 29 del Regolamento UE 2016/679, art. 2-quaterdecies del D.Lgs. 196/2003, art. 19 del D. Lgs. 51/2018), e degli operatori dell'Ente da lui autorizzati, la consultazione in tempo reale dei flussi video. Costoro possono effettuare la consultazione dei flussi tramite PC nelle postazioni operatore/workstation opportunamente dimensionate, attraverso le rispettive utenze.

Il Server ha un sistema di backup dei dati, pertanto la ridondanza dei dati avviene su un apparato Nas esterno, ubicato in luogo differente da quella dove è situato il Server.

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 Società incaricata del servizio di manutenzione e assistenza:

Riferimenti tecnici hardware:

- Telecamere Mod. TS5MPX-OCR-G o equivalente

Riferimenti tecnici software

- Server lettura targhe Targa System

Modalità di trasmissione dei dati

Le immagini riprese dalle telecamere vengono trasmesse attraverso collegamenti con linea UMTS alla Sala server sita presso il Comando della Polizia Locale.

Le immagini sono visionate in diretta dalla sala di controllo della Polizia Locale.

► **Risorse informatiche di supporto ai dati**

I flussi acquisiti dalle videocamere sono registrati in modalità cifrata su un server NVR dedicato situato presso la sala server del Comando della Polizia Locale. Il Responsabile dell'impianto e i soggetti autorizzati possono effettuare la consultazione dei flussi tramite computer a questo abilitati e dotati del necessario software, attraverso le rispettive utenze o tramite tablet che consente di fermare in tempo reale il mezzo sprovvisto di assicurazione e/o non in regola con le revisioni periodiche.

Sistema di Registrazione:

Il sistema di registrazione e conservazione dei filmati, anche nell'ottica delle finalità d'impiego da parte dell'Autorità Giudiziaria, consente:

- l'archiviazione schedulabile con Playback;
- la memorizzazione delle immagini provenienti da tutte le telecamere al massimo framerate possibile;
- l'archiviazione di flussi con algoritmo;
- la registrazione delle immagini avviene con modalità cifrata per garantirne la riservatezza e l'integrità;
- l'esportabilità (da locale o da remoto) dei filmati con corredo di specifico visualizzatore per la decifratura e verifica dell'integrità degli stessi;
- la capacità di conservazione dei dati è dimensionata per la registrazione contemporanea di tutte le telecamere al massimo frame rate consentito dalle stesse e/o dalla connettività, per un periodo di almeno 7 gg.

► **Area geografica di riferimento**

Comune di Monteleone d'Orvieto.

► **Standard applicabili al trattamento**

Nessuno

► **Tipologia di dati trattati**

Dati personali:

Immagini derivanti dalle inquadrature e/o dalle registrazioni che rendono il soggetto identificabile ex art. 4, comma 1, punto 1) del GDPR;

Dati particolari:

Nessuno

Dati giudiziari:

Nessuno

- ▶ 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?
 - ☒ Nessuna
- ▶ 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
- ▶ Il trattamento prevede attività di monitoraggio sistematico o videosorveglianza?
 - ☒ Si:
 - ☒ Videosorveglianza
- ▶ Il trattamento prevede trattamenti su larga scala?

☒ Sì, nella fattispecie si tratta di

☒ ambito geografico dell'attività di trattamento → Persone, automezzi e ciclomotori che transitano nelle aree oggetto di videosorveglianza

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

☒ No

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

☒ No

► 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

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

☒ No

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

☒ No

Responsabilità per l'utilizzo dei dati

► Chi è il titolare dei dati acquisiti?

Comune di Monteleone d'Orvieto

► Quali sono le figure interne del Titolare deputate al trattamento dei dati?

Persona autorizzata al trattamento: Responsabile dell'impianto nella persona del Comandante della Polizia Locale p.t.

Persona autorizzata al trattamento: Personale appartenente alle forze di polizia/dell'ordine e autorizzate all'accesso della sala server e al trattamento dei dati dal Titolare, qualora il Responsabile dell'impianto non sia personalmente nella sede del Comando

► I dati possono essere condivisi/trattati da soggetti terzi? E per quali finalità?

☒ Sì, nella fattispecie di tratta di:

AUTORITA' GIUDIZIARIA E FORZE DI POLIZIA: per finalità di indagine, di polizia giudiziaria e sanzionatorie. I trattamenti hanno ad oggetto tutte le immagini acquisite per le suindicate finalità.

SOCIETA' CHE SI OCCUPA DELLA MANUTENZIONE DELLE TELECAMERE: per finalità di manutenzione. I trattamenti hanno ad oggetto tutte le immagini visionate per le suindicate finalità

SOCIETA' CHE SI OCCUPA DELL'ASSISTENZA PER IL SOFTWARE: per interventi di assistenza. I trattamenti hanno ad oggetto tutte le immagini visionate per le suindicate finalità

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

► I dati potranno essere trasferiti al di fuori dell'Unione Europea?

☒ No

► I dati potranno essere condivisi con organizzazioni situate al di fuori dell'Unione Europea?

☒ No

Finalità e modalità del trattamento

► a. prevenire e reprimere atti delittuosi, attività illecite anche di tipo amministrativo 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 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 d.lvo 267/2000;

► b. acquisire automaticamente le liste aggiornate dei veicoli rubati, non assicurati o non revisionati;

► c. monitorare i flussi di traffico

► Come si prevede che i dati siano mantenuti e aggiornati?

I dati, consistenti in fotogrammi e filmati video, saranno conservati per 7 giorni sui server sopra indicati e duplicati (back up) su apparato NAS esterno ubicato in luogo differente rispetto ai locali ove è situato il server. Qualora per le finalità sopra descritte risultasse necessario al Responsabile dei trattamenti della videosorveglianza e/o a soggetti da lui incaricati acquisire copia in locale (nelle proprie postazioni) di fotogrammi e/o filmati video, questi saranno conservati fino a quando non sia conclusa l'indagine di polizia giudiziaria.

► Periodo di conservazione dei dati

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?

☒ Sì, solo informativa

L'informativa è resa all'interessato tramite:

☒ cartelli contenenti informativa breve presso i luoghi presso i quali sono collocate le videocamere

☒ altro – Informativa completa pubblicata sul sito istituzionale

La richiesta di consenso NON è dovuta in quanto:

☒ 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?

☒ Sì

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/o
- 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 in 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 (Polizia di Stato etc.);
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);
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 Polizia Locale) e dei soggetti dallo stesso incaricati;

Misure fisiche:

ricovero degli apparati di registrazione (server/NVR) in stanza chiusa con chiave;
serrature di sicurezza e porta blindata;
vigilanza della sede, (presenziamento diurno);
collocazione sala di controllo in ambiente vietato al pubblico;
estintori 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;
residenza temporanea dei dati su server e cancellazione automatica dopo 7 giorni mediante sovrascrittura;
backup dei dati su apparato Nas esterno, ubicato in luogo differente rispetto al 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
			A	B	C	D
			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 4 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: 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 tramite collegamento UMTS;
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;
- 2 Erroneo 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 del luogo in cui è ubicato il server: valutare lo stato dell'arte del luogo
Monitoraggio della temperatura e dell'umidità del luogo ove è ubicato il server
Auspicabile predisporre un sistema di allarme, allarme antincendio e fumo nel luogo è ubicato il server
Controllo periodico degli estintori nei luoghi ove è ubicato il server
Predisporre un regolamento chiavi dell'armadietto ove è contenuto il 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 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.

5. FASE IV: Conclusione della DPIA

Parere del DPO

Il DPO ritiene adeguate le misure a tutela dei diritti e delle libertà degli Interessati dichiarate dal Titolare.

Tuttavia, nel contempo, ritiene necessario stimolare un controllo sistematico e costante da parte del Titolare, in ottica di continuo miglioramento e ordinato a testare il sistema generale interno *data protection*. Il Titolare, pertanto, è invitato ad un riesame almeno annuale delle misure, per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati eseguita o quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Si suggerisce, inoltre, di adottare precise ed ulteriori istruzioni scritte nell'ipotesi in cui, in caso di vacanza o assenza del Responsabile dell'impianto, il soggetto appartenente all'amministrazione *de qua* debba per scopi di legge effettuare il trattamento in esame o darne seguito.

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.

Il Titolare dei trattamenti

Comune di Monteleone d'Orvieto

Il Sindaco
