

COMUNE DI FROSINONE



Valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del GDPR 2016/679

Indice

Quando eseguire una Valutazione d'impatto sulla protezione dei dati	2
Descrizione del trattamento	7
Dati e Valutatori	8
Validazione	10
DPO e parere degli interessati	10
Contesto	11
Principi Fondamentali	14
Misure a tutela dei diritti degli interessati	14
Rischi e Misure	16
Misure esistenti o pianificate	16

Rischi Accesso	19
Accesso illegittimo ai dati	19
Rischi Perdita	23
Perdita di dati	23
Tabella Rischi.....	24
Panoramica dei rischi	24
Tabella Gravità del Rischio	25
Tabella Impatti, Minacce, Fonti, Misure	29

Quando eseguire una Valutazione d'impatto sulla protezione dei dati

La Dpia – Data Protection Impact Assesment – è una procedura prevista dall’articolo 35 del Regolamento (UE) 2016/679 con l’obiettivo stabilire misure idonee ad affrontare i rischi in riferimento ai diritti e alle libertà delle persone fisiche di cui si effettua il trattamento dei dati.

L’articolo prevede una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare rischi elevati per gli interessati e ne specifica i casi in cui è necessaria e ne proceduralizza anche le modalità da seguire e gli elementi da tenere in considerazione. Nello specifico, il **D.lgs. 10 marzo 2023 n. 24** (che ha recepito la Direttiva 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell’Unione), all’art. 13 comma 6, prevede che venga realizzata una **valutazione di impatto sulla protezione dei dati** (DPIA).

Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Inoltre, l’art. 36 del Regolamento (UE) 2016/679 stabilisce la consultazione preventiva obbligatoria dell’Autorità di controllo quando il titolare ritiene che i trattamenti richiedano misure specifiche per attenuarne i rischi.

È inoltre utile precisare che nelle linee-guida in materia di valutazione d’impatto sulla protezione dei dati¹ il WP29² raccomanda di effettuare comunque la DPIA in tutti i casi in cui non è chiaro se sia richiesta una valutazione d’impatto sulla protezione dei dati o meno, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

Inoltre, sempre il WP29 nelle predette linee guida per la determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 ha precisato che: “*come*

¹Linee guida in materia di valutazione d’impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017.

²Gruppo dell’articolo 29 per la tutela dei dati (in inglese Article 29 Working Party o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Oggi diventato European Data Protection Board (Comitato europeo per la protezione dei dati) col nuovo Regolamento europeo ha sostituito il Gruppo di lavoro articolo 29

indicato dalle parole "in particolare" nella frase introduttiva dell'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati. Anche tali trattamenti devono essere soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati. Per questo motivo, i criteri sviluppati qui di seguito vanno, talvolta, al di là di una semplice spiegazione dell'interpretazione dei tre esempi di cui all'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati."

È poi necessario considerare che il Garante per la protezione dei dati personali italiano, circa i criteri che un Titolare deve considerare per determinare se è necessario eseguire una valutazione di impatto (DPIA), si è espresso nel seguente modo: *"Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l'autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.*

Si tratta di uno degli elementi di maggiore rilevanza del vigente quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati.

I titolari sono infatti tenuti non soltanto a garantire l'osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

Le stesse linee guida del WP29 precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all'art. 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.

Le linee-guida chiariscono, peraltro, anche quando una valutazione di impatto non sia richiesta: ciò vale, in particolare, per i trattamenti in corso che siano già stati autorizzati dalle autorità competenti e non presentino modifiche significative prima del 25 maggio 2018, data di piena applicazione del regolamento.

In sostanza le linee-guida indicano che la valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. In questo senso, la valutazione di impatto permette di realizzare concretamente l'altro fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (data protection by design) di qualsiasi trattamento."

I criteri specifici individuati dal WP29 per determinare quando la DPIA è obbligatoria sono:

- **trattamenti valutativi o di scoring**, compresa la profilazione;
- **processo decisionale automatizzato** che ha effetto giuridico o incide in modo analogo significativamente quindi decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- **monitoraggio sistematico (es: videosorveglianza)** che include i trattamenti utilizzati per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c)). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà.

Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

– **dati sensibili o dati aventi carattere altamente personale**, questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli degli indagati. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

– **trattamenti di dati personali su larga scala**, il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- c) la durata, ovvero la persistenza, dell'attività di trattamento;
- d) la portata geografica dell'attività di trattamento;

– **creazione di corrispondenze o combinazione di insiemi di dati**, combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);

– **dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio che causa un aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente

e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

- **utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);**
- **trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto** (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

Sempre il WP29 definisce la DPIA non è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

Conclusioni circa la necessità di effettuare la DPIA nel caso di specie.

Alla luce della disamina di quanto disposto dal Regolamento (UE) 2016/679 all'articolo 35 e di quanto chiarito sia dal Garante della Protezione dei dati personali italiano e a livello UE dal Gruppo dell'articolo 29 è da ritenersi necessario effettuare una valutazione di impatto (DPIA) circa il rischio elevato per i diritti e le libertà delle persone fisiche che può presentare l'adozione il sistema di “fototrappole” comunale ai fini di fronteggiare l'abbandono di rifiuti e/o l'utilizzo scorretto da parte dei cittadini delle eventuali c.d. eco-piazzole trattandosi di un sistema di videosorveglianza dedicato che può realizzare una *“sorveglianza sistematica su larga scala di una zona accessibile al pubblico” e in quanto tale possa definirsi un trattamento che “possa presentare rischi elevati ai sensi dell'articolo 35, paragrafo 3, del Regolamento (UE) 2016/679.*

Il Garante per la Protezione dei Dati Personali con l'Provvedimento generale 8 aprile 2010 in tema di videosorveglianza al **punto 5.2** si occupa dell'utilizzo di un sistema di videosorveglianza finalizzato al monitoraggio delle aree adibite a “deposito dei rifiuti”.

In particolare, il provvedimento distingue a seconda che l'impianto di videosorveglianza sia utilizzato per:

1. controllare l'utilizzo abusivo di aree impiegate come discariche di materiali e sostanze pericolose;
2. controllare il rispetto delle disposizioni (esempio ordinanze comunali) concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente ai sensi dell'art. 13, legge 24 novembre 1981, n. 689).

Prendendo in considerazione i criteri definiti dal Gruppo dell'articolo 29 per determinare l'obbligatorietà della realizzazione della DPIA pare indiscutibile che, nel caso di adozione di fototrappole, siano rilevabili “almeno due di questi criteri” potendosi compiere con tali dispositivi:

1. un processo decisionale automatizzato;
2. un monitoraggio sistematico;
3. di dati sensibili o dati aventi carattere altamente personale;
4. su larga scala;
5. che possono comprendere anche dati relativi a interessati vulnerabili;
6. e che potrebbero comprendere utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative.

Descrizione del trattamento

Il sistema di videosorveglianza è il seguente:



8012345612260



SCHEDA

A

MODELLO

ECOCAM 4.0

L'apparecchiatura per videosorveglianza ECOCAM 4.0 è costituita da un insieme di dispositivi elettronici, tra loro opportunamente collegati e interfacciati, destinati all'acquisizione video di dati per sorveglianza ambientale e alla gestione degli stessi per uso consentito dalla legge.

SCHEDA TECNICA E CARATTERISTICHE

COMPENSAZIONE CONTROLUCE	Automatico	SCAMBIO GIORNO E NOTTE	Automatico con rilevazione del filo IR CUT
CPU	HEBASIC-M323 Sony	CONNESSIONE	Rete dati 4G - Wi-Fi RJ45 Ethernet LAN 10/100 Mbps
DIMENSIONI	226 x 200 x 170 mm	SEGNALE	PAL
ZOOM	Su Focale 2,7/35 mm	VISIONE NOTTURNA IR	25 MIT
FRAME RATE VIDEO	25 FPS	PROTEZIONE	IP65 Corpo in alluminio e PVC
FREQUENZA	60Hz	AVANZAMENTO PRESET	orizzontale 300°/s; TILT 120°/s
CAMERA	>0.45	RANGE TILT E ROTAZIONE	Range 30°/s; speed 0.5/120°/s
OTTICA	Sony 2" 1/4" 8 Mpx	RANGE ORIZZONTALE E ROTAZIONE	18 Range 350°/s; speed 0.3/200°/s
IR-CUT	si	PANNELLO SOLARE	Potenza 80W - Dim. 67x36x3 cm
IR LED	6 Array Led PM 42	BATTERIA A LITO	Capacità 50Ah
MOTION DETECTION MULTI-STREAMING	si	TEMPERATURA DI FUNZIONAMENTO BATTERIA	-20°C - 60°C
ILLUMINAZIONE	0 lux	DURATA BATTERIA	Circa 1000 cicli di carica
PROTOCOLLI	TCP UDP RTP HTTP RTSP ONVIF APP: ICMP POP RTSP SIP	AUTONOMIA BATTERIA PER ECOCAM 4.0	72 Ore
POEL	3840x2160 4K	PESO	16.5 Kg
MAIN STREAM	1080p@30fps 720p@30fps 2 Mpx HD	MISURE IMBALLO	780x705x222 cm
RICONOSCIMENTO UMANO	si (Notifica dedicata) NEW	MODULO GPS (OPZIONALE)	



CON TIPO TRACKER, 12 MAGNETI
SENSORE ANTI-SABOTAGGIO AUTO ALIMENTATO CON
BATTERIA RICORDIA
AUTONOMIA IN STANDBY 300 ORE

MEPA
acquisti@mepea.it
Ecocam4.0

ECOCAM 4.0

ECOCAM 4.0

SISTEMA DI VIDEOSORVEGLIANZA AUTONOMO

Kit elettronico intelligente pronto all'uso che consente di videosorvegliare luoghi esterni dove non c'è né la corrente né una connessione Internet. Nata per sorveglianza ambientale e gestione della stessa per uso consentito dalla legge.

Prodotto da
SimplyNet S.r.l.



Via Maringo Alto, 57
03027 Rieti (FR)



(+39) 0775 1638262
Mobile (+39) 395 2900205



ISO 9001



ISO 14001



ISO 27001



AON



Service SaaS qualificato sul
CLOUD MARKETPLACE AON



Dati e Valutatori

Ente: Comune di Frosinone

Sezione:

Redattore dell'Analisi: Arch. Giuseppe Viscogliosi - Dirigente Settore Ambiente e Mobilità -

Valutatore dell'analisi: Dott. Riccardo Mastrangeli

DPO Comune Frosinone: Dott. Enrica Popolla

DPO Comune Frosinone: Stato Valutazione 100%

- Validazione dell'Analisi dei rischi
- Validazione del Piano d'azione

Principi fondamentali

Nessuna azione/misura correttiva

Misure esistenti o pianificate

Nessuna azione/misura correttiva

Rischi

Nessun piano d'azione registrato

Validazione

DPO e parere degli interessati

Nome del DPO/RPD

Dott. Enrica Popolla

Posizione del DPO/RPD

Il trattamento può essere implementato

Parere del DPO/RPD

Seppure il tipo di trattamento in sé possa rappresentare un rischio relativo ai diritti e libertà dei soggetti interessati qualificabile come elevato, si ritiene che i dispositivi e le misure tecniche ed organizzative individuate e adottate fin dalla progettazione che saranno utilizzate durante l'esercizio sono da ritenersi adeguate a mitigare il rischio portando il rischio residuale ad un livello che può essere qualificato come "residuale basso".

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si ritiene utile per questo trattamento richiedere il parere degli interessati in quanto la base giuridica del trattamento eseguito con le fototrappole, ai sensi dell'art. 6, comma 1, lettera e) del Reg. UE 2016/679 è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Questa DPIA è atta alla valutazione dell'impatto connesso all'uso di nuove tecnologie al fine di rilevare immagini catturate attraverso l'utilizzo di fototrappole gestite in outsourcing per poi poter comminare sanzioni amministrative contro l'abbandono illegittimo dei rifiuti nelle periferie del Comune di Frosinone, nonché per la tutela della pubblica sicurezza, prevenzione e accertamento di reati. Nella presente DPIA sono presi in considerazione i trattamenti di dati personali operati per mezzo di tecnologie che permettono le rilevazioni di filmati/immagini degli interessati nonché numero di targhe di veicoli con i quali vengono abbandonati illegittimamente i rifiuti nelle aree di proprietà del Comune di Frosinone.

Quali sono le responsabilità connesse al trattamento?

Il Comune di Frosinone è il Titolare del trattamento

Simplynet s.r.l. è Responsabile del trattamento per la fornitura e la gestione del sistema di fototrappole.

Ci sono standard applicabili al trattamento?

Attualmente non sono stati rinvenuti standard, certificazioni o codici di condotta applicabili al trattamento.

L'intero processo è stato qualificato da ACN, l'Agenzia responsabile dei Servizi Cloud e delle Infrastrutture dei Servizi Cloud della Pubblica Amministrazione.

Valutazione: Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati comuni; immagini di persone e cose (automobili, targhe ecc.) che consentono l'identificazione degli interessati.

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

Per ciclo di vita del dato s'intende l'insieme delle fasi in cui un dato si può trovare durante la sua esistenza ovverosia:

- a) **la raccolta:** il ciclo di vita inizia con la raccolta delle informazioni. I dati possono entrare nel perimetro comunale;
- b) **il salvataggio:** una volta che i dati sono entrati all'interno del perimetro comunale dovranno essere memorizzati in appositi luoghi fisici e/o virtuali in modo tale che poi possano essere utilizzati;
- c) **l'analisi:** in questa fase si analizzano gli esiti dell'attività di raccolta per determinare la qualità dei dati da utilizzare. Vi è quindi un confronto tra *output desiderato* e *output effettivo* per, eventualmente, pianificare migliorie e attività correttive che abbiano impatti sulle fasi precedenti;
- d) **il filtraggio dei dati:** in seguito agli esiti dei risultati della fase c), i dati vengono filtrati e modificati in modo da rispecchiare gli *output desiderati*;
- e) **l'utilizzo:** in questa fase i dati vengono effettivamente utilizzati per comminare le sanzioni amministrative;
- f) **l'archiviazione:** in questa fase i dati vengono memorizzati in attesa di essere dismessi e/o riutilizzati;
- g) **la cancellazione o anonimizzazione:** in questa fase il periodo di conservazione è ormai scaduto e quindi: o si cancella il dato personale, oppure lo si rende anonimo. Deve essere evitato, in questa fase, ricorso alla pseudonimizzazione, che porterebbe, come noto, a generare dati destinati ad essere trattati al pari dei personali.

Quali sono le risorse di supporto ai dati?

L'accesso ai dati e ai frame selezionati è consentito esclusivamente alla centrale operativa di SimplyNet S.r.l. quindi al personale interno alla Società autorizzato al trattamento per le attività tecniche e di gestione del servizio, nonché al personale comunale della Polizia Locale formalmente autorizzato per le attività di verifica, accertamento e gestione dei procedimenti conseguenti, nel rispetto dei profili di autorizzazione attribuiti.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Tenuto conto della normativa di riferimento si precisa che la base giuridica del trattamento eseguito con le fototrappole, ai sensi dell'articolo 6, comma 1, lettera e) del Regolamento (UE) 2016/679 è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento; il pubblico interesse tutelato si può sostanziare nel perseguimento della sicurezza urbana, come definita dall'art. 4 del DL 14/2017, nell'accertamento e prevenzione degli illeciti in materia di deposito non conforme dei rifiuti.

In particolare, il sistema di videosorveglianza mobile è finalizzato ad accertare **l'utilizzo abusivo di aree impiegate come discariche** di materiali e di sostanze pericolose, nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologia di orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente. Le riprese filmate e l'estrazione dei fotogrammi per l'accertamento degli illeciti ambientali possono riguardare sia le violazioni contemplate nel Testo Unico Ambientale, D.lgs. 152/2006 (utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose con riflessi penali e/o amministrativi a seconda delle norme violate e delle relative sanzioni stabilite) sia le violazioni amministrative alle disposizioni emanate dall'Ente comunale (corretto conferimento dei rifiuti).

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 196/2003 (Codice Privacy);

Decreto Legislativo 18 agosto 2000, n. 267 "*Testo unico delle leggi sull'ordinamento degli enti locali*";

Decreto legislativo 3 aprile 2006, n. 152 *Norme in materia ambientale* (in particolare artt. 192, 255 e 256);

Legge n. 689/1981;

Provvedimento del garante in materia di videosorveglianza – 8 APRILE 2010 (punto 5.2 “Deposito dei rifiuti”);

D.L. n. 14/2017 “Disposizioni urgenti in materia di sicurezza della città”;

Linee guida EDPB N. 3/2019;

Regolamenti interni e piani di intervento del Comune in questo ambito.

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 personali acquisiti con le fototrappole consistono in video/immagini dei volti degli interessati, targhe di veicoli e tipologia di veicolo appartenenti agli interessati nonché video contenuti nelle

registrazioni acquisite mediante le foto trappole installate in determinate zone all'interno del comune di Frosinone.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

I dati sono esatti e aggiornati in quanto vengono rilevati con l'ausilio di fototrappole regolarmente mantenute e i software utilizzati vengono costantemente aggiornati.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Se i dati oggetto di trattamento sono pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti vengono successivamente trattati, nonché conservati per 72 ore dal momento della registrazione. Potranno essere conservati per un periodo superiore a 72 ore - in una forma che consenta l'identificazione dell'interessato e che ne garantisca la sicurezza e la riservatezza - qualora i medesimi dati costituiscano prove di illecito amministrativo e/o elementi probatori per l'accertamento e/o perseguimento dei reati. Se invece i dati non sono completi e/o utili alla finalità in oggetto, allora saranno cancellati entro i sette giorni dal ricevimento

Valutazione: Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

In conformità a quanto disposto dagli artt. 13-14 del GDPR gli interessati sono messi al corrente dell'utilizzo di foto trappole in determinate aree del comune di Frosinone attraverso l'affissione di appositi cartelli di videosorveglianza nonché di relativa informativa entrambi posizionati a debita distanza dal "cono di ripresa" della foto trappola nonché attraverso l'informativa pubblicata sul sito istituzionale dell'ente.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Non è previsto il consenso da parte degli interessati in quanto il trattamento rientra tra i compiti di interesse pubblico di cui è investito il Titolare.

Valutazione: Accettabile

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

Con l'informativa posizionata posizionati a debita distanza dal "cono di ripresa" nonché attraverso l'informativa pubblicata sul sito istituzionale del comune di Frosinone, l'interessato viene messo a conoscenza delle del fatto che in qualunque momento, potrà esercitare il proprio diritto di accesso alle informazioni (art.15e art. 11 D. Lgs. 51/2018) mediante comunicazione scritta da inviare all'indirizzo email dpo@comune.frosinone.it, mediante pec da inviare all'indirizzo pec@pec.comune.frosinone.it oppure a mezzo raccomandata all'indirizzo del Titolare del trattamento dei dati (Piazza VI Dicembre - Palazzo Comunale,– 03100 – FROSINONE).

Non è possibile per l'interessato esercitare il diritto alla portabilità ai sensi dell'art. 20 del GDPR, in quanto è un trattamento 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 e come tale escluso dalla possibilità di esercizio di tale diritto dal punto 3 dello stesso articolo.

Valutazione: Accettabile

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

Con l'informativa posizionata posizionati a debita distanza dal "cono di ripresa" nonché attraverso l'informativa pubblicata sul sito istituzionale del comune di Frosinone, l'interessato viene messo a conoscenza delle del fatto che in qualunque momento, potrà esercitare i propri diritti di rettifica (art.16 e art. 12 c.1 D. Lgs. 51/2018) e di cancellazione (art. 17 e art. 12 c.2 D. Lgs. 51/2018) mediante comunicazione scritta da inviare all'indirizzo email dpo@comune.frosinone.it, mediante pec da inviare all'indirizzo pec@pec.comune.frosinone.it oppure a mezzo raccomandata all'indirizzo del Titolare del trattamento dei dati (Piazza VI Dicembre - Palazzo Comunale,– 03100 – FROSINONE).

Valutazione: Accettabile

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

Con l'informativa posizionata posizionati a debita distanza dal "cono di ripresa" nonché attraverso l'informativa pubblicata sul sito istituzionale del comune di Frosinone, l'interessato viene messo a conoscenza delle del fatto che in qualunque momento, potrà esercitare i propri diritti di limitazione di trattamento (art. 18 e art. 12 c.3 D. Lgs. 51/2018), di opposizione (art.21) e relativo al processo decisionale automatizzato, compresa la profilazione (art. 22 GDPR e art. 8 D. Lgs. 51/2018) mediante comunicazione scritta da inviare all'indirizzo email dpo@comune.frosinone.it, mediante pec da inviare all'indirizzo pec@pec.comune.frosinone.it oppure a mezzo raccomandata all'indirizzo del Titolare del trattamento dei dati (Piazza VI Dicembre - Palazzo Comunale,– 03100 – FROSINONE).

Valutazione: Accettabile

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

Il Titolare del trattamento ha nominato un Responsabile esterno del trattamento i cui obblighi dei sono definiti con chiarezza e disciplinati con atto di nomina (contratto) ai sensi e per gli effetti del art. 28 Reg. UE 2016/679.

Valutazione: Accettabile

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

I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

Valutazione: Accettabile

Rischi e Misure

Misure esistenti o pianificate

Le misure tecniche ed organizzative implementate sono le seguenti:

- **Cifratura**
- **Controllo accessi**
- **Capacità di ripristinare disponibilità e accesso ai dati**
- **Antivirus**
- **Credenziali di accesso**
- **Scadenza password**
- **Formazione/istruzione personale**
- **Policy e procedure specifiche**

In particolare, la Simplynet srl garantisce quanto segue:

Fascia oraria di attivazione dell'impianto		L'impianto è attivo h 24.
Caratteristiche tecniche delle telecamere interne ed esterne installate e loro posizionamento e inquadratura.		Vedasi scheda tecnica degli apparati messa a disposizione dal fornitore (Allegato 1). L'inquadratura viene limitata alle sole aree di interesse ed il posizionamento è sulle aree di scarica o deposito dei rifiuti da parte dei cittadini.
Modalità di funzionamento del dispositivo di registrazione		I dispositivi operano riprendendo le immagini limitrofe ai luoghi di scarica.
Profilazione dei livelli di accesso	Adozione di un sistema di autenticazione che permetta di effettuare, a seconda dei compiti attribuiti ad ogni soggetto autorizzato, unicamente le operazioni di propria competenza.	Livelli di profilazione al momento sono tutti uguali tra loro.
Limitazione alla cancellazione o duplicazione delle immagini	Deve essere limitata la possibilità, per i soggetti autorizzati di effettuare sulle videoriprese operazioni di cancellazione o duplicazione.	Solo gli operatori Simplynet possono accedere alla gestione del pannello di controllo delle telecamere.

Periodo di conservazione delle immagini	Adozione di misure tecniche o organizzative per la cancellazione anche in forma automatica, delle registrazioni allo scadere del termine previsto. Cfr. Linee guida 3/2019 sul Trattamento dei dati personali mediante apparati video Faq dell'Autorità di Controllo sul tema e dei recenti Provvedimenti sul tema (Cfr. Ordinanza 9 giugno 2022, n. 214).	72 h a seguito delle quali c'è una sovrascrizione - Di norma le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite (art.5 Gdpr). Spetta al Titolare del trattamento (Comune) individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. In osservanza dell'art. 6, co. 8, del D.L. 23/02/2009, n. 11, l'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza pubblica urbana, è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione. Simplynet S.r.l. in osservanza dei principi del Gdpr non imposta tempi di conservazione superiori alle 72h a meno che non vi sia una richiesta specifica, giustificata dalla base giuridica, da parte del Comune Titolare del trattamento. Si sottolinea a tal proposito che, più è prolungato il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione.
Specifiche cautele in caso di interventi di manutenzione	I soggetti preposti possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali modifiche tecniche e in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini.	La visione delle immagini è limitata ai soli soggetti autorizzati dotati di username e password di accesso. I dipendenti Simplynet hanno la possibilità di accedere anche per scopi di manutenzione e monitoraggio delle risorse e verifica delle funzionalità generali.
Protezione degli apparati di ripresa digitali connessi a reti informatiche	Devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del Codice Penale.	E' presente l'accesso solo mediante autenticazione con Username e Password.
Misure di sicurezza di immagini tramite una rete pubblica di comunicazioni.	Deve essere effettuata previa applicazione di tecnologie crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessione wireless.	La trasmissione dati avviene con scheda Sim che trasferisce i dati al server mediante i canali del gestore.
Designazione incaricati	Il titolare e il Responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad accedere ai locali dove sono situate le postazioni di controllo sia ad utilizzare gli impianti, e nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.	Simplynet ha proceduto a nominare quale autorizzati al trattamento i propri dipendenti che trattano dati personali.

Controllo degli accessi	Il Titolare deve verificare la protezione dei locali dove sono posizionati i monitor per le riprese video da accessi non autorizzati. I monitor devono essere fruibili solo ai soggetti autorizzati.	La Simplynet ha una propria sala CED accessibile solo ai soggetti autorizzati.
Sicurezza dei supporti	Il Titolare deve prevedere idonee misure di sicurezza per i supporti sui quali le immagini vengono salvate. (se presenti)	Dopo aver ricevuto un link, il committente o suo delegato sarà reindirizzato a uno spazio di archiviazione contenente i file elaborati. L'attività di gestione dati si svolgerà interamente presso la Centrale Operativa della Simplynet videosorveglianza. L'intero processo è stato qualificato da ACN, l'Agenzia responsabile dei Servizi Cloud e delle Infrastrutture dei Servizi Cloud della Pubblica Amministrazione.
Registro degli accessi	Il titolare deve monitorare il registro degli accessi ai file delle riprese dell'impianto di videosorveglianza.	E' presente un registro degli accessi ai dati delle riprese di videosorveglianza che indichi chi ha effettuato l'accesso e in quale data.
Verifica della operatività del Sistema	Monitoraggio e individuazione dei guasti in modo continuativo con previsione di alert in caso di malfunzionamento o carenze anche per tempi brevi.	Il sistema viene monitorato costantemente dagli operatori Simplynet. A richiesta del titolare del trattamento è possibile installare un ulteriore modulo Gps in caso di sottrazione della telecamera con atti vandalici.
Designazione dei Responsabili	Nomina ex art. 28	Simplynet ha un contratto di manutenzione e quindi una volta effettuato il collaudo può accedere alle immagini di videosorveglianza.

Rischi Accesso

Accesso illegittimo ai dati

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

Violazione della riservatezza di dati personali comuni e/o sensibili, comunicazione/diffusione dei dati non autorizzata, conoscenza da parte di terzi del fatto che è stata posta in essere una condotta costituente illecito amministrativo, interferenza su abitudini, interferenza su vita privata.

Qualora fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza, i dati sarebbero crittografati, quindi si tratterebbe di un impatto limitato

Valutazione: Accettabile.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso abusivo ai sistemi, malware, hacker, cancellazione involontaria, distruzione del dispositivo, furto del dispositivo, cancellazione volontaria

Valutazione: Accettabile.

Quali sono le fonti di rischio?

Un soggetto autorizzato che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. Terzi che fanno un accesso abusivo ai sistemi. Sistemi automatici di accesso abusivo al sistema

Valutazione: Accettabile.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Cifratura
- Controllo accessi
- Capacità di ripristinare disponibilità e accesso ai dati
- Antivirus
- Credenziali di accesso
- Scadenza password
- Formazione/istruzione personale
- Policy e procedure specifiche

Valutazione: Accettabile.

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

La quantità e la rilevanza dei dati personali trattati potrebbe comportare una gravità di rischio che può essere considerata trascurabile, sulla base delle misure pianificate.

Valutazione: Accettabile.

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

La quantità e la rilevanza dei dati personali trattati potrebbe comportare una probabilità di rischio che può essere considerata Trascurabile, sulla base delle misure pianificate.

Valutazione: Accettabile

Rischi Modifica

Modifiche indesiderate dei dati

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

Conoscenza da parte di terzi del fatto che è stata posta in essere una condotta costituente illecito amministrativo, Cancellazione parziale dati, individuazione errata destinatari provvedimenti, non attribuzione di un illecito commesso.

Valutazione: Accettabile.

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

Accesso abusivo ai sistemi, hacker, malware, furto del dispositivo, errore materiale

Valutazione: Accettabile.

Quali sono le fonti di rischio?

Un soggetto autorizzato che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. Terzi che fanno un accesso abusivo ai sistemi, Errore umano, Fonti umane interne, che intervengano nella modifica dei dati.

Valutazione: Accettabile.

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

- Cifratura
- Controllo accessi
- Capacità di ripristinare disponibilità e accesso ai dati
- Antivirus
- Credenziali di accesso
- Scadenza password
- Formazione/istruzione personale
- Policy e procedure specifiche

Valutazione: Accettabile.

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

Trascurabile, in quanto, ebbene la violazione potrebbe portare ad una errata o inefficace prestazione del servizio, le misure di controllo degli accessi permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.

Valutazione: Accettabile

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

Trascurabile, in quanto, appare marginale che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda alla corretta applicazione e gestione delle misure di sicurezze adottate e pianificate dal comune di Frosinone.

Valutazione: Accettabile

Rischi Perdita

Perdita di dati

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

Violazione della riservatezza di dati personali comuni e/o sensibili, comunicazione/diffusione dei dati non autorizzata, conoscenza da parte di terzi del fatto che è stata posta in essere una condotta costituente illecito amministrativo, interferenza su abitudini, interferenza su vita privata

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso abusivo ai sistemi, malware, hacker, cancellazione involontaria, distruzione del dispositivo, furto del dispositivo, cancellazione volontaria

Quali sono le fonti di rischio?

Un soggetto autorizzato che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. Terzi che fanno un accesso abusivo ai sistemi.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Cifratura
- Controllo accessi
- Capacità di ripristinare disponibilità e accesso ai dati
- Antivirus
- Credenziali di accesso
- Scadenza password
- Formazione/istruzione personale
- Policy e procedure specifiche

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

La quantità e la rilevanza dei dati personali trattati potrebbe comportare una gravità di rischio che può essere considerata trascurabile. La divulgazione di dati personali di cui il comune di Frosinone è titolare, anche ex Art. 9 e 10 GDPR, potrebbe avere conseguenze negative sugli interessati.

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

La quantità e la rilevanza dei dati personali trattati potrebbe comportare una probabilità di rischio che può essere considerata Trascurabile, sulla base delle misure pianificate.

Valutazione: Accettabile

Tabella Rischi

Panoramica dei rischi

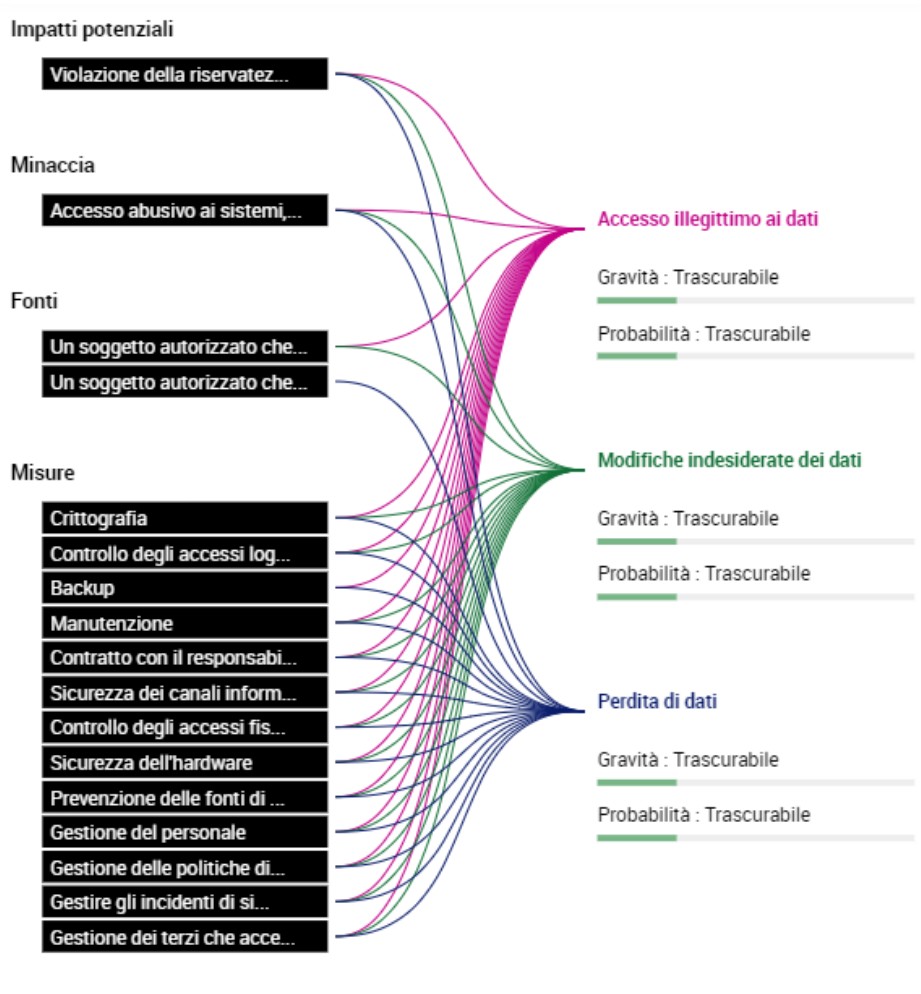


Tabella Gravità del Rischio

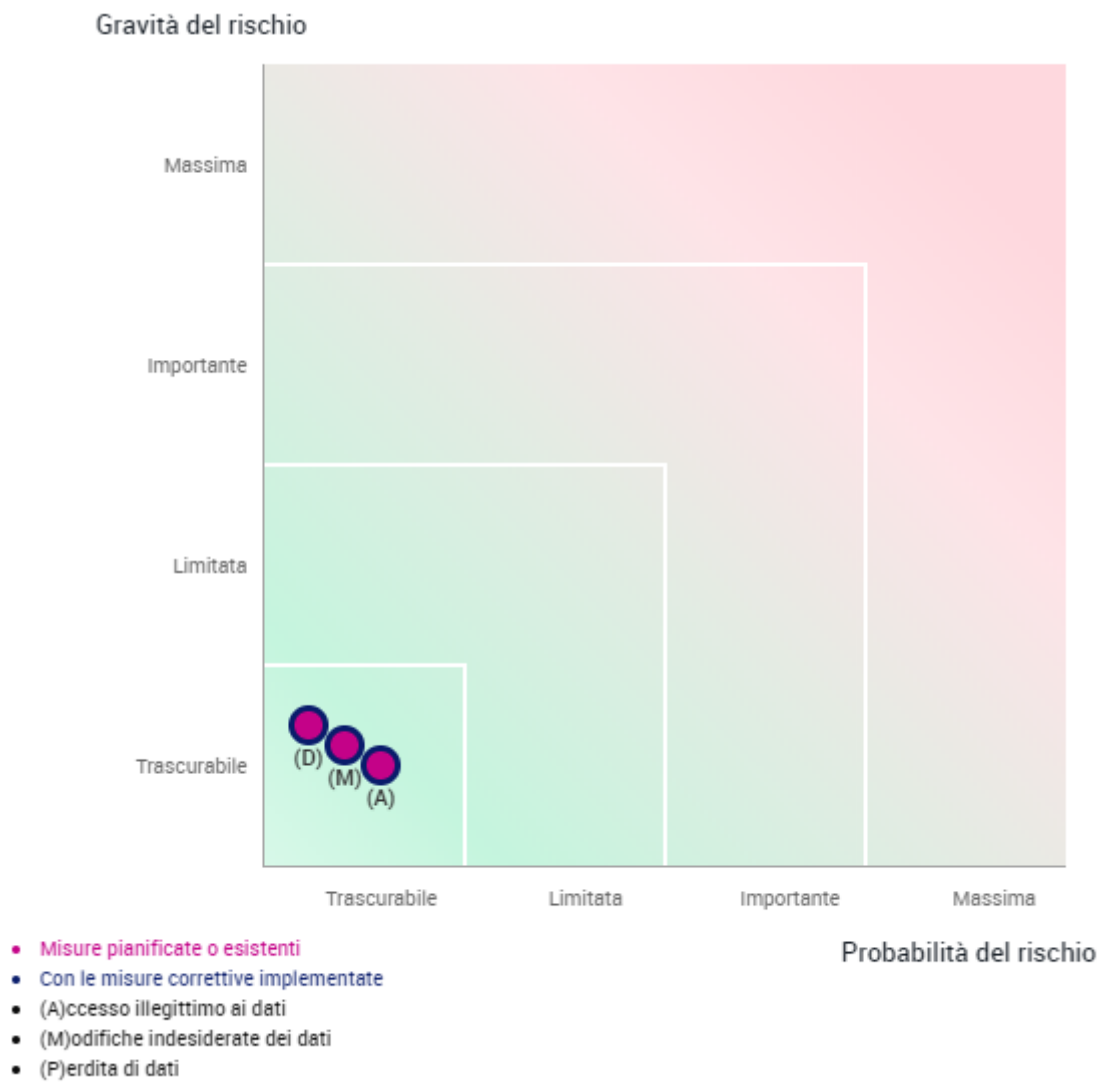


Tabella Impatti, Minacce, Fonti, Misure

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 dei dati

Misure esistenti o pianificate

- ☐ Crittografia
- ☐ Controllo degli accessi logici
- ☐ Backup
- ☐ Manutenzione
- ☐ Contratto con il responsabile del trattamento
- ☐ Sicurezza dei canali informatici
- ☐ Controllo degli accessi fisici
- ☐ Sicurezza dell'hardware
- ☐ Prevenzione delle fonti di rischio
- ☐ Gestione del personale
- ☐ Gestione delle politiche di tutela della privacy
- ☐ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- ☐ Gestione dei terzi che accedono ai dati
- ☐ Sicurezza dei documenti cartacei

Rischi

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

Allegati:

1. SCHEDA TECNICA - ECOCAM 4.0
2. MODALITA' DI ESECUZIONE DI VIDEOANALISI
3. DPIA SIMPLYNET SRL_Rev2025
4. RELAZIONE POSIZIONAMENTO TELECAMERE

Frosinone, 25/06/2026

Il redattore e validatore dell'analisi

Arch. Giuseppe Viscogliosi

GIUSEPPE
VISCGLIOSI
01.07.2026
15:31:48
GMT+02:00



Il validatore dell'analisi

Dott. Riccardo Mastrangeli

RICCARDO
MASTRANGELI
02.07.2026
12:14:40
GMT+02:00



per il parere di competenza

Il DPO

Dott.ssa Enrica Popolla