VIDEOSORVEGLIANZA URBANA

DATA PROTECTION IMPACT ASSESSEMENT

Comune di Vittuone

Città Metropolitana di Milano

4 NOVEMBRE 2024

REL. 1.0

Sommario

Documenti di riferimento

N. ALLEGATO	DESCRIZIONE	NOME FILE
01	Disciplinare tecnico di istruzione per il trattamento di videosorveglianza	ALLEGATO 01 DPIA - DISCIPLINARE TECNICO DI ISTRUZIONE PER IL TRATTAMENTO DI VIDEOSORVEGLIANZA DI CONTESTO.docx
02	Disciplinare tecnico di istruzione per il trattamento di lettura targhe	ALLEGATO 02 DPIA - DISCIPLINARE TECNICO DI ISTRUZIONE PER IL TRATTAMENTO DI VIDEOSORVEGLIANZA DI LETTURA TARGHE.docx
03	Disciplinare tecnico di istruzione per l'impiego di sistemi di videosorveglianza fototrappole	ALLEGATO 03 DPIA - DISCIPLINARE TECNICO DI ISTRUZIONE PER L'IMPIEGO DI SISTEMI DI VIDEOSORVEGLIANZA FOTOTRAPPOLE.docx
04	Disciplinare tecnico di istruzione per l'impiego del sistema di rilevazione "rosso semaforico"	ALLEGATO 04 DPIA - DISCIPLINARE TECNICO DI ISTRUZIONE PER L'IMPIEGO DI SISTEMA ROSSO SEMAFORICO.docx
05	Facsimile registri	ALLEGATO 05 DPIA - FACSIMILE REGISTRI.docx
06	Tool Calcolo HASH	ALLEGATO 06 DPIA - Calcolo HASH.zip

Premessa

La Dpia – Data Protection Impact Assesment – è una procedura prevista dall'articolo 35 del Regolamento (UE) 2016/679.

La valutazione d'impatto della protezione dei dati (DPIA) serve a descrivere un trattamento di dati per valutarne la necessità, la proporzionalità e i relativi rischi.

L'obiettivo è quello di 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.

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

Il Regolamento (UE) 2016/679 fa riferimento all'obbligo del titolare di tenere conto dei rischi che i trattamenti possono comportare per i diritti e le libertà delle persone:

- nell'art.24, che individua l'analisi dei rischi fra le caratteristiche dei trattamenti di cui occorre tener conto per mettere in atto tutte le misure tecniche e organizzative adeguate indicando che il Titolare deve sempre essere in grado di dimostrare di aver adottato tutte le misure necessarie affinché il trattamento sia conforme al Regolamento;
- nell'art. 35, che prevede una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare rischi elevati per gli interessati, specifica i casi in cui è necessaria e procedimentalizza le modalità da seguire e gli elementi da tenere in considerazione;

  l'art.35 prevede inoltre un ruolo molto rilevante delle Autorità di controllo, che possono redigere e rendere pubblico un elenco delle tipologie di trattamenti per i quali è richiesta comunque la valutazione di impatto (art. 35, 4); così come possono, se lo ritengono opportuno, redigere un elenco delle tipologie di trattamenti per i quali essa non è necessaria.
- nell'art.36 che stabilisce la consultazione preventiva obbligatoria dell'Autorità di controllo quando il titolare ritiene che i trattamenti richiedano misure specifiche per attenuarne i rischi.

Nel concreto quindi per ogni trattamento è necessario effettuare un'analisi dei rischi (art.24) finalizzata all'accertamento del livello di rischio per poter, a valle di questa valutazione, decidere se il rischio per i cittadini sia elevato o meno e quindi se è necessario procedere con una valutazione di impatto per l'individuazione delle misure specifiche da adottare (art. 35) per minimizzare il rischio e se del caso successivamente procedere con una consultazione preventiva dell'Autorità di controllo.

Rispetto a come deve essere effettuata una DPIA è d'aiuto ricorrere a quanto indicato dal WP29[1] nelle linee guida[2] in materia di valutazione d'impatto sulla protezione dei dati personali, da cui si ricavano preziose indicazioni:

- l'analisi dei rischi relativi a un trattamento va fatta sempre prima che questo inizi;
- l'analisi va fatta rispetto a ciascun singolo trattamento, salvo il caso di trattamenti simili;
- deve essere prestata attenzione sul piano tecnologico anche alle componenti dei dispositivi utilizzati;
- ogni analisi deve tener conto dei casi di cui all'art. 35 nonché delle specifiche indicate ai punti 71, 75 e 91 dei Considerando;
- deve essere svolta con una metodologia che tenga conto dei criteri e degli elementi indicati nell'annex 2 delle Linee guida.

Nel caso in cui al termine dell'analisi condotta secondo la metodologia indicata nelle Linee guida il titolare, sentito il DPO, ritenga che non sussistano rischi elevati può limitarsi a dare applicazione a quanto richiesto dall'art. 24.

Tuttavia, il WP29 precisa che anche in questo caso il titolare deve giustificare per iscritto le valutazioni fatte e tenere un registro dei trattamenti svolti sotto la sua responsabilità.

Quando, all'esito dell'analisi svolta nell'ambito della DPIA, risultino rischi elevati per gli interessati, il titolare deve adottare misure tecniche adeguate a minimizzare il rischio.

Le linee guida non contengono indicazioni specifiche su questo punto, in quanto aventi contenuto ed obiettivi essenzialmente procedurali; va considerato inoltre che la DPIA è un processo continuo, una valutazione che deve essere costantemente aggiornata al modificarsi delle condizioni di esercizio.

Spetta perciò al titolare individuare le misure di sicurezza o altre modalità di riduzione del rischio da adottare, sentito il DPO se nominato. Il titolare può anche consultare gli interessati o i loro rappresentanti dandone atto nel documento scritto che costituisce la parte formale della DPIA.

Nel documento è bene anche indicare i soggetti che hanno svolto l'analisi dei trattamenti e individuato le misure necessarie.

Per quanto riguarda la metodologia relativa all'individuazione delle misure idonee a diminuire i rischi, le linee guida si limitano a fissare i criteri da seguire, distinguendo tra quelle che hanno come obiettivo principale la riduzione del rischio e quelle finalizzate a dimostrare la conformità con il Regolamento.

[1] Gruppo 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.

[2] Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) - https://ec.europa.eu/newsroom/article29/items/611236

Per quanto riguarda i casi in cui si debba consultare preventivamente l'Autorità le Linee guida indicano che il ricorso alla consultazione dell'Autorità di controllo è necessario solo quando il titolare "non riesce a individuare misure sufficienti per ridurre i rischi a un livello accettabile.

Necessità di effettuare una valutazione di impatto (DPIA) preventiva per adozione di impianti di videosorveglianza comunale ai fini di sicurezza urbana

La DPIA è da considerarsi obbligatoria per quanto riguarda gli impianti di videosorveglianza impiegati dai Comuni ai fini di sicurezza urbana per i motivi esposti di seguito.

In primo luogo è da considerare il fatto che l'applicazione del Regolamento (UE) sulla protezione dei dati personali si basa sul principio di accountability che in concreto vuole dire che il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

È quindi utile chiarire che il regolamento generale sulla protezione dei dati **non** richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche.

La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "*possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (articolo 35, paragrafo 1, illustrato dall'articolo 35, paragrafo 3, e integrato dall'articolo 35, paragrafo 4).

È inoltre utile precisare che il WP29[3] 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

[3] Gruppo 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.

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.

È altrettanto utile ricordare che l'articolo 35, paragrafo 3, del Regolamento (UE) 2016/679 fornisce alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati":

a) *"una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
b) *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*
c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*".

Inoltre, sempre il WP29 nelle linee guida in materia di valutazione d'impatto sulla protezione dei dati per la determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 ha precisato che:

"come 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, riguardo ai 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 linee-guida[4] del WP29[5] offrono alcuni chiarimenti sul punto; in particolare, 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 Gruppo Art. 29 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 generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate in grado di aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati sensibili (nel senso

[4] Linee 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.

[5] Gruppo 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.

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 vengano 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[6];
- 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 in grado di opporsi e consentire 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).

[6] NdR – Sempre in relazione alla popolazione di riferimento

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 Gruppo Art. 29 ha precisato che 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 ritersi 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 di un sistema di videosorveglianza comunale ai fini di sicurezza urbana[7], trattandosi di un sistema che può realizzare una *"sorveglianza sistematica su larga scala di una zona accessibile al pubblico"* e, in quanto tale, può definirsi un trattamento che *"possa presentare rischi elevati ai sensi dell'articolo 35, paragrafo 3, del Regolamento (UE) 2016/679*".

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 un impianto di videosorveglianza comunale ai fini di sicurezza urbana, siano rilevabili "almeno due di questi criteri" potendosi compiere con tale impianto:

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

[7] D.Lgs. 14/2017 "… si intende per sicurezza urbana il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, la promozione del rispetto della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile, cui concorrono prioritariamente, anche con interventi integrati, lo Stato, le Regioni e Province autonome di Trento e Bolzano e gli enti locali, nel rispetto delle rispettiva competenze e funzioni"

Metodologia utilizzata

La valutazione d'impatto sulla protezione dei dati deve tenere conto del rischio complessivo che il trattamento previsto può comportare per i diritti e le libertà degli interessati, alla luce dello specifico contesto.

Pertanto, il concetto di rischio non si esaurisce nella considerazione delle possibili violazioni o minacce della sicurezza dei dati.

È quindi un processo complesso che deve tenere in considerazione e valutare i diversi aspetti tecnici ed organizzativi necessari a minimizzare, fino a renderli accettabili, il possibile impatto sulle persone del trattamento che si intende effettuare, in relazione ai loro diritti e alle loro libertà.

Per effettuare la valutazione di impatto si è seguito il metodo definito dalla CNIL – Autorità francese per la protezione dei dati – con il supporto del software di ausilio ai titolari per l'effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA) messo a punto dalla stessa autorità e la cui versione in lingua italiana è stata messa a punto con la collaborazione del Garante Italiano della protezione dei dati personali.

Il software offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29[8] nelle Linee-guida sulla DPIA[9].

Facilita lo svolgimento di una valutazione d'impatto sulla protezione dei dati, seguendo la metodologia definite dalle guide PIA pubblicate dalla CNIL.

Lo strumento rappresenta una base di conoscenze giuridiche e tecniche e comprende le basi legali che garantiscono la liceità del trattamento e i diritti degli interessati.

Tale valutazione complessiva effettuata utilizzando la metodologia CNIL è stata integrata con una metodologia specifica per il calco del rischio sulle tre aree di impatto riservatezza, integrità e disponibilità riferite alle rispettive minacce quali l'accesso Illegittimo, le modifiche indesiderate e la perdita di dati

La valutazione dei rischi è il primo passo verso l'adozione di adeguate misure di sicurezza per la protezione dei dati personali.

La DPIA è da considerarsi il presente documento nel suo complesso, corredato da tutti gli allegati che ne sono parte integrante.

8 Gruppo 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.

9 Linee 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.

Validazione

TIPOLOGIA DI IMPIANTI PRESENTI	
TIPOLOGIA	**PRESENZA**
VIDEOSORVEGLIANZA WIRELESS	Sì
VIDEOSORVEGLIANZA CABLATO	Sì
VIDEOSORVEGLIANZA INTEGRATA	No
VARCHI RILEVAMENTO TARGHE	Sì
FOTOTRAPPOLE	Sì
RILEVAMENTO ROSSO SEMAFORICO	Sì
BODYCAM	No
DASHCAM	No
DRONI	No

Schema del sistema

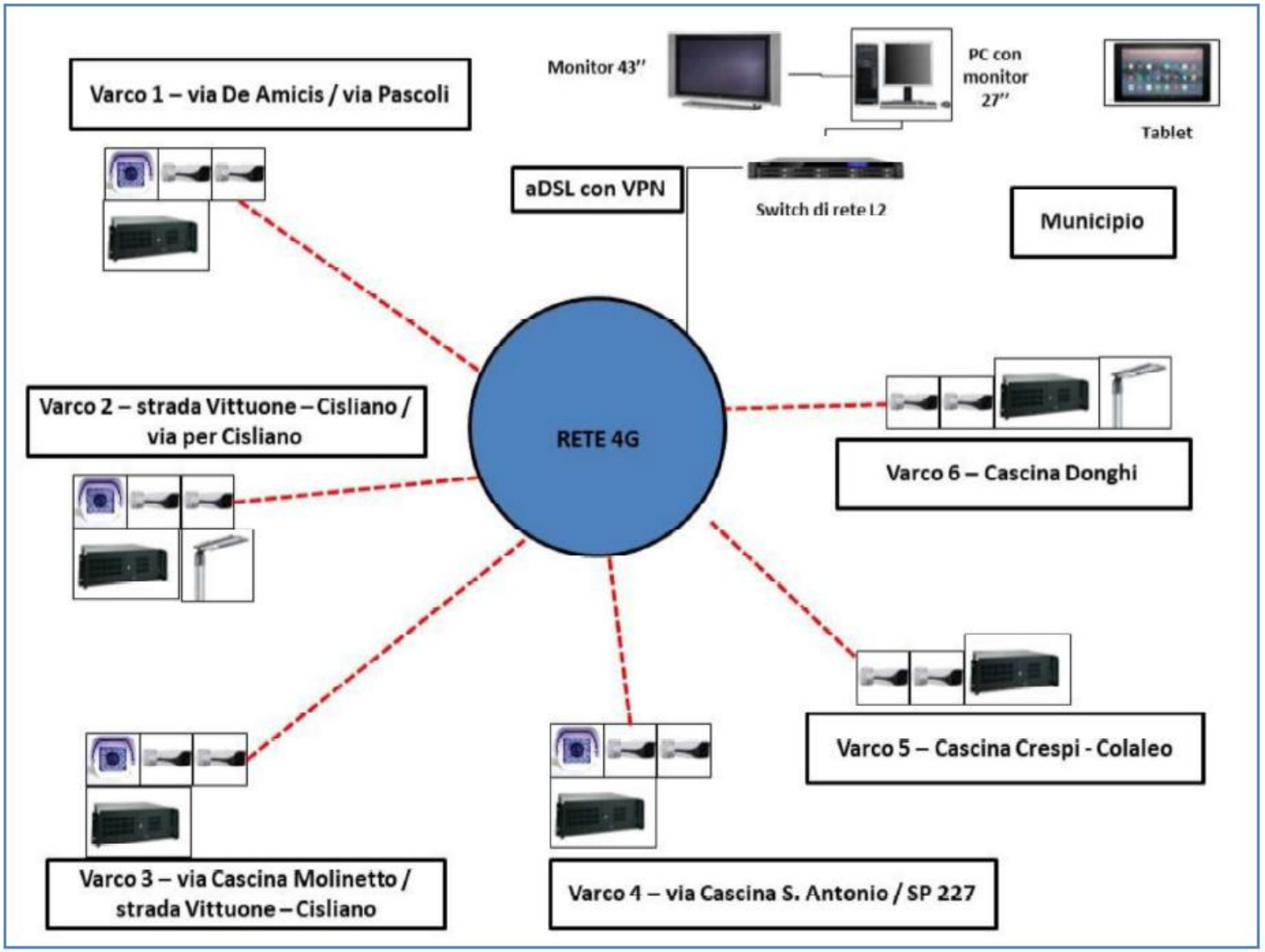


Tabelle di sintesi delle caratteristiche degli impianti e configurazioni

Impianto di videosorveglianza

CARATTERISTICHE DEL SISTEMA DI VIDEOSORVEGLIANZA		
TITOLO	**VALORE**	**ANNOTAZIONI**
Numero telecamere	32 Ambientali	
Marche e modelli	Hikvision/TMC	
Numero NVR/DVR/SERVER	6 NVR + 1 NVR (centrale)	Le telecamere ubicate in Piazza Italia, P.zza Venini e Via Santi Nazaro Celso (vecchio impianto) sono ubicate sul Palazzo Comunale e scaricano direttamente sul NVR presente c/o sala CED del Comune
Marca	HikVision	
Numero postazioni di visualizzazione	1	Ubicata presso l'ufficio del Comandante
Sistema operativo delle postazioni di visualizzazione	Windows 11 PRO	
Sistema software di gestione della videosorveglianza	HikVision IVMS 4200	
Sistema operativo del server di videosorveglianza		non c'è server, ma NVR
Server in Cloud o In house	In House	NVR Fisici
Servizio Cloud o SaaS qualificato AgID/ANC		
Gestione del servizio interno o esterno	Interno	
Attività esternalizzate	Altro (specificare)	Al momento l'impianto è in fase di avviamento, pertanto non ancora attivo il contratto di manutenzione. La ditta che segue l'avviamento del nuovo sistema (telecamere NON ubicate sul Palazzo Comunale) interviene anche sul vecchio sistema. Ditta SKP Tecnology -p.iva 07799690966 Via Ripamonti, 66 – 20141 Milano

CARATTERISTICHE DELLA RETE UTILIZZATA DAL SISTEMA DI VIDEOSORVEGLIANZA		
TITOLO	**VALORE**	**ANNOTAZIONI**
Rete del sistema di videosorveglianza	Sì	Presente Vlan dedicata
Infrastruttura di trasmissione dei dati	Altro (specificare)	Rete Vlan per le telecamere ubicate sul palazzo comunale e linea ADSL con VPN protetta, firewall e credenziali di accesso alla piattaforma HikConnect che consente il collegamento con i diversi NVR dislocati sul territorio
Tecnologia/Protocollo/Frequenza di trasmissione (se wireless)		
Possibilità di accedere al sistema dall'esterno della rete dell'impianto di videosorveglianza	No	
Misure di sicurezza adottate per consentire l'accesso dall'esterno della rete		Al momento non è possibile il collegamento dall'esterno.

GESTIONE CREDENZIALI DI ACCESSO AL SISTEMA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Credenziali personali per accedere al sistema	Sì	Unico utente con password complesse e cambio periodico obbligato
Custodia delle credenziali	Ognuno conserva per se	
Presenza di un gruppo di utenti abilitato alla sola gestione immagini live	No	

GESTIONE CREDENZIALI DI ACCESSO AL SISTEMA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Presenza di un gruppo di utenti abilitato solo alla gestione delle immagini registrate e da esportare	No	
Presenza di un gruppo di utenti abilitato sia alla gestione delle immagini live, sia alla gestione delle immagini registrate e da esportare	Sì	Personale del Comando
Presenza gruppo amministratore	Sì	Ditta SKP Tecnology

B.4 - GESTIONE PROTEZIONE FISICA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Le apparecchiature dei siti esterni sono all'interno di armadi stradali in vetroresina chiusi con serrature personalizzate	Sì	Apertura con unica chiave standard a triangolo
Le apparecchiature all'interno di edifici sono collocate in armadi e locali ad accesso limitato e controllato secondo le policy di sicurezza in uso	Sì	Le apparecchiature sono ubicate su palo ad eccezione di quelle del vecchio impianto che sono ubicate al soffitto del portico o sul tetto del Palazzo Comunale
I server sono all'interno del locale CED ad accesso controllato per il solo personale autorizzato	Sì	Gli NVR esterni sono ubicati su Pali ad altezza non raggiungibile se non con scala. L'NVR ubicato presso il Comune è in Sala CED chiuso a chiave accessibile al solo responsabile del CED
I pc client sono all'interno del comando di Polizia Locale in locali non accessibili al pubblico e dedicati al servizio di controllo e vigilanza	No	Il PC di visualizzazione è ubicato presso ufficio del comandante, locale accessibile ai colleghi, non chiuso, ma con chiavi
Le infrastrutture di terze parti sono garantite dalle società che erogano i servizi secondo i contratti in essere	No	Non ci sono strutture esterne

Impianto di lettura targhe

CARATTERISTICHE DEL SISTEMA DI LETTURA TARGHE		
TITOLO	**VALORE**	**ANNOTAZIONI**
Numero telecamere del sistema di lettura targhe	4 OCR	
Marche e modelli delle telecamere per la lettura targhe	HikVision TCM	
Numero NVR/DVR/SERVER del sistema di lettura targhe	1 PC Server	Ubicato presso la sala CED del Comune - stesso PC utilizzato per la visualizzazione vds
Marca e modello NVR/DVR/SERVER del sistema di l. targhe	WINBLU-287586	
Numero postazioni di visualizzazione dedicate alla l. targhe	1	Presso l'ufficio del Comandante
Sistema operativo delle postazioni di visualizzazione dedicate alla l. targhe	Windows 11 PRO	
Sistema software di gestione della lettura targhe	Traffic Scanner	
Sistema operativo del server del sistema di l. targhe	Windows 11 PRO	
Server in Cloud o In house	In House	
Servizio Cloud o SaaS qualificato AGID/ANC		Server Fisico
Gestione del servizio interno o esterno	Interno	
Attività esternalizzate	Solo manutenzione	
OCR - Riconoscimento automatico delle targhe	Sì	

CARATTERISTICHE DEL SISTEMA DI LETTURA TARGHE		
TITOLO	**VALORE**	**ANNOTAZIONI**
Comparazione in tempo reale dei dati delle targhe rilevate con quelli presenti in sistemi informatici di diversa natura e tipologia (es. SCNTT)	No	Non Presente
Dati delle targhe archiviati per fini di indagine e statistici	Sì	
Alert in tempo reale agli operati in caso di veicoli segnalati e/o non in regola con assicurazione e/o revisione	No	
Utilizzo Alert da postazione fissa e/o mobile (tablet)	No	Non Presente
Gestione Whitelist	Sì	
Gestione Blacklist	Sì	
Omologazione del MIT per la contestazione delle violazioni	No	

CARATTERISTICHE DELLA RETE UTILIZZATA DAL SISTEMA DI LETTURA TARGHE		
TITOLO	**VALORE**	**ANNOTAZIONI**
Rete del sistema di lettura targhe dedicata	Sì	Stessa rete della VDS di contesto
Infrastruttura di trasmissione dei dati	Altro (specificare)	
Tecnologia/Protocollo/Frequenza di trasmissione (se wireless)		
Possibilità di accedere al sistema dall'esterno della rete dell'impianto di lettura targhe	Sì	tramite IP Pubblico inserendo User e Password. Sul server è possibile l'accesso tramite teamviewer con psw fornita di volta in volta dal comandante. Accesso dall'esterno per la sola manutenzione
Misure di sicurezza adottate per consentire l'accesso dall'esterno della rete	Verifica IP	

GESTIONE CREDENZIALI DI ACCESSO AL SISTEMA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Credenziali personali per accedere al sistema	Sì	Unico utente con password complesse e cambio periodico obbligato
Custodia delle credenziali	Ognuno conserva per se	
Presenza di un gruppo di utenti abilitato alla sola gestione immagini live	No	
Presenza di un gruppo di utenti abilitato solo alla gestione delle immagini registrate e da esportare	No	
Presenza di un gruppo di utenti abilitato si alla gestione delle immagini live, sia alla gestione delle immagini registrate e da esportare	Sì	Personale del Comando
Presenza gruppo amministratore	Sì	Ditta SKP Tecnology

GESTIONE PROTEZIONE FISICA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Le apparecchiature dei siti esterni sono all'interno di armadi stradali in vetroresina chiusi con serrature personalizzate	Sì	Apertura con unica chiave standard a triangolo
Le apparecchiature all'interno di edifici sono collocate in armadi e locali ad accesso limitato e controllato secondo le policy di sicurezza in uso	Sì	Le apparecchiature sono ubicate su palo ad eccezione di quelle del vecchio impianto che sono ubicate al soffitto del portico o sul tetto del Palazzo Comunale
I server sono all'interno del locale ced ad accesso controllato per il solo personale autorizzato	Sì	Gli NVR esterni sono ubicati su Pali ad altezza non raggiungibile se non con scala. L'NVR ubicato presso il Comune è in Sala CED chiuso a chiave accessibile al solo responsabile del CED
I pc client sono all'interno del comando di Polizia Locale in locali non accessibili al pubblico e dedicati al servizio di controllo e vigilanza	No	Il PC di visualizzazione è ubicato presso ufficio del comandante, locale accessibile ai colleghi, non chiuso, ma con chiavi
Le infrastrutture di terze parti sono garantite dalle società che erogano i servizi secondo i contratti in essere	No	non ci sono strutture esterne

Fototrappole

CARATTERISTICHE DEL SISTEMA DI FOTOTRAPPOLE		
TITOLO	**VALORE**	**ANNOTAZIONI**
Numero telecamere del sistema di FOTOTRAPPOLE	7	
Marche e modelli delle telecamere per le FOTOTRAPPOLE	2 Geotech flex e 5 Geotech AFC	
Numero NVR/DVR/SERVER del sistema di FOTOTRAPPOLE	NA	
Marca e modello NVR/DVR/SERVER del sistema di FOTOTRAPPOLE	NA	
Numero postazioni di visualizzazione dedicate alle FOTOTRAPPOLE	1	Lo scarico della SD viene fatta sul PC del Comandante manualmente a cura del Comandante
Sistema operativo delle postazioni di visualizzazione dedicate alla FOTOTRAPPOLE	Windows 11 pro	
Sistema software di gestione della FOTOTRAPPOLE	Non presente	Le immagini sono decriptate con il programma CryptoAFC fornito dalla casa costruttrice delle fototrappole
Sistema operativo del server del sistema di FOTOTRAPPOLE	WINDOWS 11 PRO	PC Comandante
Server in Cloud o In house	In House	
Servizio Cloud o SaaS qualificato AgID/ANC		
Gestione del servizio interno o esterno	Interno	Le fototrappole sono gestite da personale del Comando, lo scarico della SD avviene manualmente a cura del Comandante
Attività esternalizzate	No	
OCR	No	
SCNTT	No	
Tipologia di protezione fisica della FOTOTRAPPOLA	Su palo al non raggiungibili	
SD CARD criptata	Sì	

GESTIONE CREDENZIALI DI ACCESSO AL SISTEMA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Credenziali personali per accedere al sistema	Sì	Credenziali pc comandante con password complesse (Combinazione di lettere maiuscole, lettere minuscole, numeri e simboli) con cambio obbligato ogni 90 giorni.
Custodia delle credenziali	Ognuno conserva per se	
Presenza di un gruppo di utenti abilitato alla sola gestione immagini live	No	
Presenza di un gruppo di utenti abilitato solo alla gestione delle immagini registrate e da esportare	No	
Presenza di un gruppo di utenti abilitato si alla gestione delle immagini live, sia alla gestione delle immagini registrate e da esportare	Sì	
Presenza gruppo amministratore	No	

D.4 - GESTIONE PROTEZIONE FISICA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Le apparecchiature dei siti esterni sono all'interno di armadi stradali in vetroresina chiusi con serrature personalizzate	Sì	
Le apparecchiature all'interno di edifici sono collocati in armadi e locali ad accesso limitato e controllato secondo le policy di sicurezza in uso	Sì	
I server sono all'interno del locale ced ad accesso controllato per il solo personale autorizzato	Sì	
I pc client sono all'interno del comando di Polizia Locale in locali non accessibili al pubblico e dedicati al servizio di controllo e vigilanza	No	Collocato in ufficio del Comandante – in fase di individuazione nuovo locale chiuso con accesso controllato da destinare alla videosorveglianza.
Le infrastrutture di terze parti sono garantite dalle società che erogano i servizi secondo i contratti in essere	Sì	

Impianto rilevamento rosso semaforico

CARATTERISTICHE DEL SISTEMA DI RILEVAMENTO ROSSO SEMAFORICO		
TITOLO	**VALORE**	**ANNOTAZIONI**
Numero telecamere del sistema	1	
Marche e modelli delle telecamere	PARVC	Project Automation -
Numero NVR/DVR/SERVER del sistema		in cloud
Marca e modello NVR/DVR/SERVER		
Numero postazioni di visualizzazione	1	
Sistema operativo delle postazioni di visualizzazione	Windows 11 Pro	
Sistema software di gestione	SRI-ENT 4.0	
Sistema operativo del server del sistema		
Server in Cloud o In house	in cloud	su Cloud Microsoft Azure (contrattualizzato da Project Automation)

CARATTERISTICHE DEL SISTEMA DI RILEVAMENTO ROSSO SEMAFORICO		
TITOLO	**VALORE**	**ANNOTAZIONI**
Servizio Cloud o SaaS qualificato AgID/ANC		
Gestione del servizio interno o esterno	Esterno	
Attività esternalizzate	Servizio cloud	Project Automation SPA
OCR - Riconoscimento automatico delle targhe	Presente	
Comparazione in tempo reale dei dati delle targhe rilevate con quelli presenti in sistemi informatici di diversa natura e tipologia (es. SCNTT)		
Dati delle targhe archiviati per fini di indagine e statistici		
Alert in tempo reale agli operati in caso di veicoli segnalati e/o non in regola con assicurazione e/o revisione		
Utilizzo Alert da postazione fissa e/o mobile (tablet)		
Gestione Whitelist		
Gestione Blacklist		
Omologazione del MIT per la contestazione delle violazioni		

CARATTERISTICHE DELLA RETE UTILIZZATA DAL SISTEMA ROSSO SEMAFORICO		
TITOLO	**VALORE**	**ANNOTAZIONI**
Rete del sistema dedicata	Linea di Comunicazione UMTS	VPN IPSEC IN TUNNEL MODE dal dispositivo di rilevamento delle infrazioni semaforiche al centro
Infrastruttura di trasmissione dei dati		
Tecnologia/Protocollo/Frequenza di trasmissione (se wireless)		
Possibilità di accedere al sistema dall'esterno della rete dell'impianto		
Misure di sicurezza adottate per consentire l'accesso dall'esterno della rete		

GESTIONE CREDENZIALI DI ACCESSO AL SISTEMA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Credenziali personali per accedere al sistema	Presente	Con password complesse e cambio obbligato ogni 90 giorni - la password di accesso alla VPN SSL per il cloud è personale a doppio fattore.
Custodia delle credenziali	Ognuno conserva per sé	
Presenza di un gruppo di utenti abilitato alla sola gestione immagini live	No	
Presenza di un gruppo di utenti abilitato solo alla gestione delle immagini registrate e da esportare	No	
Presenza di un gruppo di utenti abilitato si alla gestione delle immagini live, sia alla gestione delle immagini registrate e da esportare	Sì	Comandante + 2 persone del Comando che in fase di individuazione
Presenza gruppo amministratore	Sì	Project Automation

GESTIONE PROTEZIONE FISICA		
MISURA	**PRESENZA**	**ANNOTAZIONI**
Le apparecchiature dei siti esterni sono all'interno di armadi stradali in vetroresina chiusi con serrature personalizzate	Altro	In custodia con grado di protezione IP66 e posizionato ad altezza tra i 4 e 5 metri.
Le apparecchiature all'interno di edifici sono collocati in armadi e locali ad accesso limitato e controllato secondo le policy di sicurezza in uso	Non presenti	
I server sono all'interno del locale CED ad accesso controllato per il solo personale autorizzato	Cloud	
I pc client sono all'interno del comando di Polizia Locale in locali non accessibili al pubblico e dedicati al servizio di controllo e vigilanza		
Le infrastrutture di terze parti sono garantite dalle società che erogano i servizi secondo i contratti in essere	Sì	

Descrizione dell'impianto

Descrizione generale

L'impianto esistente consiste in 32 telecamere di contesto, 4 telecamere di lettura targhe, 7 fototrappole, 1 sistema di rilevamento rosso semaforico.

Le telecamere ubicate sul palazzo comunale sono collegate al Comando attraverso una rete Vlan dedicata. Le comunicazioni tra siti esterni e Comando sono realizzate con appoggio su rete 4G, dovuto alla difficoltà di impostare delle tratte di connessione in visibilità ottica diretta. Di conseguenza, per il rispetto delle indicazioni ai sensi della privacy, si è fatto ricorso a collegamenti VPN protetti.

Architettura del sistema

Sistema di Videosorveglianza

Il sistema di videosorveglianza si appoggia alla piattaforma iVMS-4200 installata sull'NVR ubicato presso il Comando. La piattaforma iVMS-4200 utilizza la tecnologia Cloud P2P per connettere i dispositivi dalla rete pubblica.

Le postazioni di videosorveglianza sono realizzate su 6 ubicazioni sparse sul territorio oltre al palazzo comunale e sono state configurate con telecamere ambientali dotate di ottica varifocale utile ad ottimizzare l'inquadratura dell'area interessata.

Le comunicazioni tra postazioni di ripresa e Comando sono realizzate appoggiandosi alla rete 4G. La scelta di questa modalità è dovuta alle difficoltà di impostare delle tratte di comunicazione in visibilità ottica diretta, condizione necessaria per il ricorso alle tecnologie radio. I collegamenti utilizzano VPN protette.

Le comunicazioni tra le postazioni di Piazza Italia (palazzo comunale) e il NVR presso il CED del Comune sono realizzate tramite cavi di rete in quanto la distanza è sempre inferiore a 100 m. Fa eccezione la postazione con 2 tc su edificio comunale di piazza Venini che ha una distanza dal NVR superiore a 100 mt, pertanto il collegamento si realizza attraverso 2

ponti radio che consentono di triangolare i flussi delle immagini acquisite al NVR del Comune.

I filmati di contesto/videosorveglianza sono registrati su NVR locali, per poi essere consultabili dal Comando secondo le necessità.

La consultazione è operata attraverso il pc Windows 11 Pro ubicato presso l'ufficio del Comandante.

Le caratteristiche del sistema ivms-4200 sono visionabili all'indirizzo https://www.hikvision.com/it/products/software/ivms-4200/.

Sistema di lettura targhe mobile

Il sistema di lettura targhe si basa su piattaforma TRAFFIC SCANNER installata sul server WINBLU-287586 ubicato nel CED del Comune e si completa con 4 telecamere presenti sul territorio integrate a telecamere di contesto.

Le comunicazioni tra postazioni e Comando sono realizzate appoggiandosi alla rete 4G tramite linea ADSL e relativo firewall.

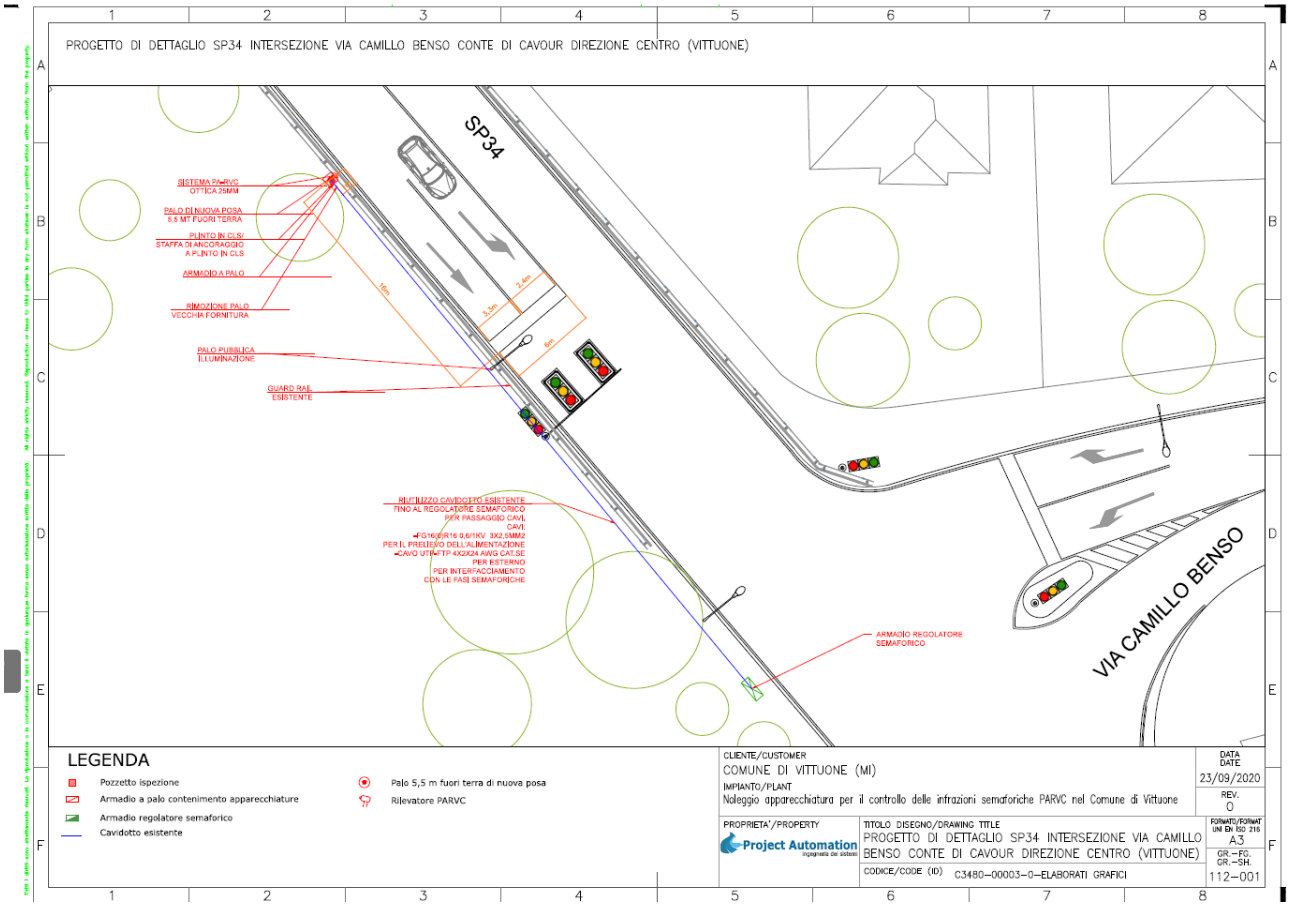
I fotogrammi relativi alle letture delle targhe sono registrati sul server del Comando.

Sistema di rilevamento rosso semaforico

L'impianto si basa su infrastruttura di tipo UMTS (con VPN IPSEC IN TUNNEL MODE) con sistema di ripresa PARVC collegato ad un server in Cloud (AZURE di Microsoft).

L'impianto è basato su sistema di ripresa PARVC (Project Automation Red Violation Control), sistema approvato dal Ministero delle Infrastrutture e dei Trasporti con Decreto n. 1929 del 3.4.2013. PARVC è costituito da un unico corpo camera che racchiude, al proprio interno, una fotocamera digitale b/n (telecamera OCR) per la ripresa video (VR-S1131), una fotocamera digitale a colori (telecamera di contesto) di tipo termico per rilevare il passaggio dei veicoli (RV-FLIR1), un illuminatore IR a LED, una unità di elaborazione e archiviazione, un sistema GPS e un sistema di gestione degli I/O e delle comunicazioni.

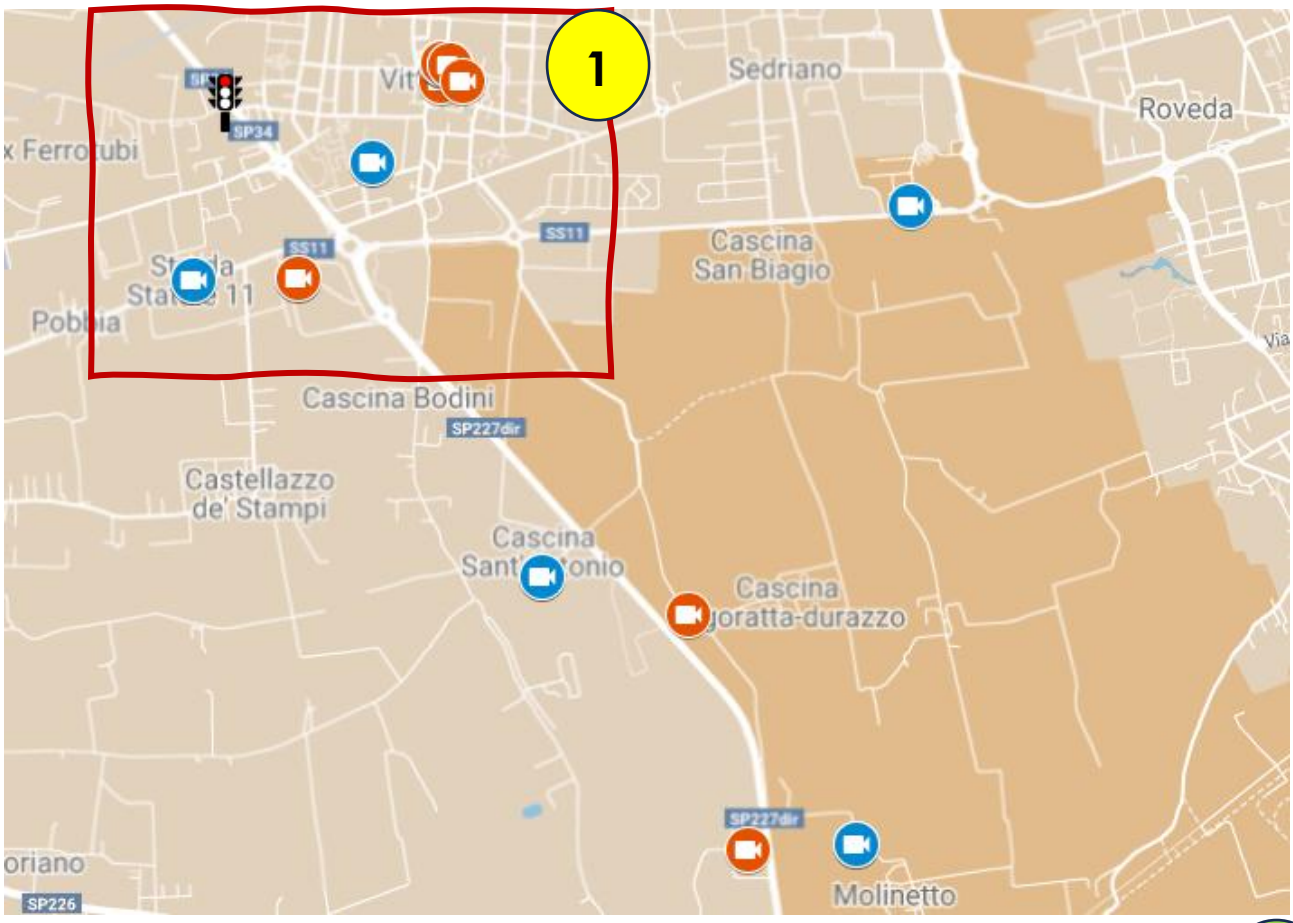
Il sistema di ripresa PARVC è dotato di memoria di sistema interna (SD card) per contenere i dati/fotogrammi con transiti in infrazione che periodicamente invia attraverso una linea di comunicazione UMTS al server cloud (AZURE di Microsoft.

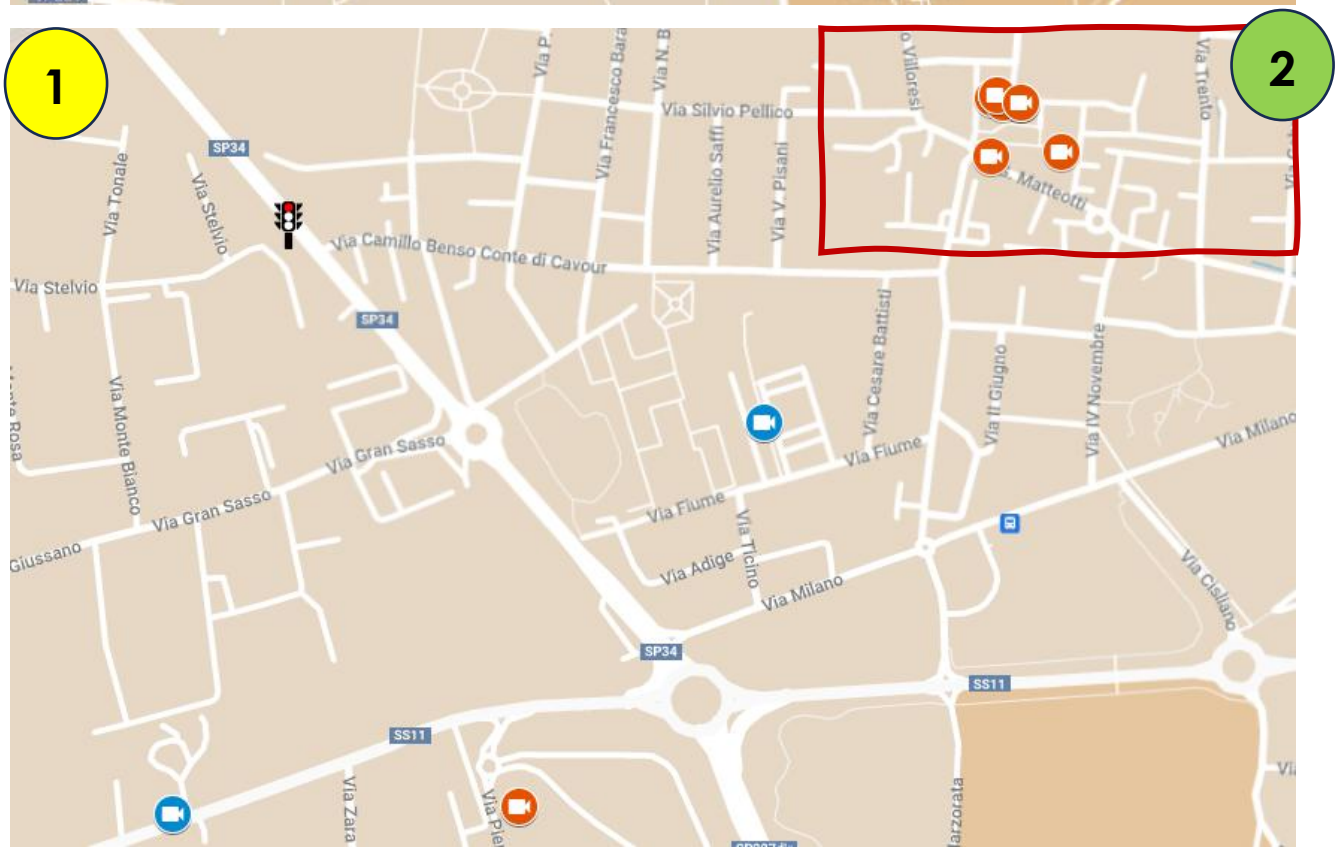


FOTOINSERIMENTO SP34 INTERSEZIONE VIA CAMILLO BENSO CONTE DI CAVOUR DIREZIONE CENTRO (VITTUONE)

Collocazione sul territorio

Impianti di videosorveglianza






2
Via Francesco Petrarca
Via Dante Alighieri
Via Francesco Petrarca
Piazza Italia
Piazza Italia
Piazza Venini
Via Giovanni Venini
Piazza Italia
Via S. Nazaro e Celso
Via S. Nazaro e Celso
Via G. Matteotti
Via Giampiero Pozzi
Via G. Matteotti
Via G. Matteotti
Via Giovanni Venini
Via Giovanni Venini

Immagini dei dispositivi

TELECAMERA HIKVISION/TCM 203


TELECAMERA HIKVISION / Color V.U. 2,8 mm


TELECAMERA HIKVISION / MICRODOME Color V.U. 2,8 mm

TELECAMERA ARECONT VISION

NVR HIKVISION

FOTOTRAPPOLA GEOTECH FLEX

FOTOTRAPPOLA GEOTECH AFC

SISTEMA RILEVAZIONE ROSSO SEMAFORICO P@RVC

Elenco dispositivi impianto videosorveglianza urbana

#	LUOGO	TIPOLOGIA	MARCA	MODELLO	CONNESSIONE
1	Via De Amicis/Pascoli	NVR + 3 telecamere	Hikvision Bulet	2- mod.TCM 203 A-B - 1- Color V.U. 2,8 mm	Wireless
2	Via per Cisliano snc - cascina crespi	NVR +2 telecamere	Hikvision Bulet	Color V.U. 2,8 mm	Wireless
3	Via Cascina Donghi 1	NVR + 2 telecamere	Hikvision Bulet	Color V.U. 2,8 mm	Wireless
4	Via Cascina Molinetto	NVR + 4 telecamere	Hikvision Bulet	2 - mod.TCM 203 A-B - 2 - Color V.U. 2,8 mm	Wireless
5	Via per Cisliano snc (chiesetta del Lazzaretto)	NVR + 4 telecamere	Hikvision Bulet	2 - mod.TCM 203 A-B - 2 - Color V.U. 2,8 mm	Wireless
6	Via Cascina Sant'Antonio	NVR + 4 telecamere	Hikvision Bulet	2 - mod.TCM 203 A-B - 2 - Color V.U. 2,8 mm	Wireless
7	Piazza Italia angolo Chiesa	1 telecamera	Hikvision Bulet	Color V.U 2,8 mm	Cablata
8	Piazza Italia angolo banca	1 telecamera	Hikvision Bulet	Microdome Color V.U. 2,8 mm	Cablata
9	Piazza Italia ingresso municipio	1 telecamera	Hikvision Bulet	Microdome Color V.U. 2,8 mm	Cablata
10	Piazza Italia ingresso teatro	1 telecamera	Hikvision Bulet	Microdome Color V.U. 2,8 mm	Cablata
11	Piazza Italia/via Dante	1 telecamera	Hikvision Bulet	Color V.U. 2,8 mm	Cablata
12	Piazza Italia alto	1 telecamera	Hikvision Bulet	Color V.U. 2,8 mm	Cablata
13	Piazza Italia retro Teatro	2 telecamera	Hikvision Bulet	Microdome Color V.U. 2,8 mm	Cablata
14	Piazza Italia portico	1 telecamera quadriottica	Arecont Vision	**Non rilevato**	Cablata
15	Piazza Pozzi su su Palazzo Comunale	1 telecamera quadriottica	Arecont Vision	**Non rilevato**	Cablata
16	piazza Venini su Palazzo Comunale	1 telecamera quadriottica	Arecont Vision	**Non rilevato**	Cablata
17	via Santi Nazaro Celso su Palazzo Comunale	2 telecamere	Hikvision Bulet	1 Color V.U. 2,8 mm - 1 Microdome Color V.U. 2,8 mm	Cablata

Elenco dispositivi sistema di lettura targhe

#	LUOGO	TIPOLOGIA	MARCA	MODELLO	CONNESSIONE
1	Via De Amicis/Pascoli	TELECAMERA OCR	HIKVISION	TMC203 A-B	WIRELESS
2	Via Cascina Molinetto	TELECAMERA OCR	HIKVISION	TMC203 A-B	WIRELESS
3	Via per Cisliano snc (chiesetta del Lazzaretto)	TELECAMERA OCR	HIKVISION	TMC203 A-B	WIRELESS
4	Via Cascina Sant'Antonio	TELECAMERA OCR	HIKVISION	TMC203 A-B	WIRELESS

Autorizzati al trattamento

Gli autorizzati al trattamento dati sono esclusivamente:

- Autorizzati interni polizia locale

Responsabili Esterni e Amministratori di Sistema

La ditta incarica della manutenzione ordinaria, correttiva ed evolutiva dell'hardware e del software dell'impianto di videosorveglianza e del sistema di lettura targhe è stata individuata ed è stato sottoscritto l'atto di nomina a resp. esterno del trattamento designato ed è:

- SKP Tecnology -P.IVA 07799690966 Via Ripamonti, 66 – 20141 Milano

È in corso di formalizzazione l'atto di nomina ad Amministratore di Sistema in capo alla stessa ditta SKP Tecnology.

Per le fototrappole non è attivo alcun contratto di manutenzione.

Per il sistema di rilevazione del rosso semaforico è attivo il contratto di manutenzione ed il contratto ed è stato sottoscritto l'atto di nomina a responsabile esterno per il servizio di cloud delle riprese in capo a:

Project Automation – P.IVA 03483920173 - viale Elvezia, 42 20900 Monza (MB)

Mappatura dei rischi

Le tre principali minacce che sono state individuate sono:

1. accesso illegittimo ai dati (riservatezza)
2. modifiche indesiderate dei dati (integrità)
3. perdita dei dati (disponibilità)

Per ogni potenziale minaccia è stata effettuata un'analisi che ha portato:

1. all'individuazione dei potenziali impatti sugli interessati che potrebbero essere prodotti al verificarsi delle minacce
2. alla stima del potenziale impatto (gravità) che il verificarsi di una determinata minaccia genererebbe
3. alla stima della probabilità che un determinata minaccia si possa verificare, ottenuta dalla pesatura della probabilità che una serie accadimenti possano verificarsi

L'impatto è classificato nel seguente modo:

IMPATTO		
Livello		Descrizione
1	Trascurabile (Lieve)	Gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente, superabile senza difficoltà
2	Limitato (Medio)	Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà.
3	Importante (Grave)	Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative
4	Massimo (Gravissimo)	Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

La probabilità è classificata nel seguente modo:

PROBABILITA'		
Livello		Descrizione
1	Trascurabile (Improbabile)	Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti
2	Limitato (Poco probabile)	Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti
3	Importante (Probabile)	Appare possibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti
4	Massimo (Altamente proba	Appare estremamente facile per le fonti di rischio considerate concretizzare una minaccia basandosi sulle caratteristiche dei supporti

Il rischio è classificato nel seguente modo:

RISCHIO		
Livello		Descrizione
1-2	Basso	Il rischio può essere considerato di livello basso
3-4	Medio	Il rischio può essere considerato di livello medio
5-8	Alto	Il rischio può essere considerato di livello alto
9-16	Altissimo	Il rischio può essere considerato di livello altissimo

Il livello di rischio è calcolato con la seguente formula:

RISCHIO = IMPATTO * PROBABILITA'

Una volta calcolato il rischio iniziale è stato effettuato il calcolo del rischio residuo calcolando la forza di mitigazione che hanno le misure di mitigazione in essere per il trattamento preso in considerazione attraverso la pesatura di ogni singola misura sia per quanto riguarda la mitigazione dell'impatto sia per quanto riguarda la mitigazione della probabilità.

Di seguito vengono illustrati i singoli passaggi effettuati per il calcolo del rischio.

Mappatura dei rischi per videosorveglianza

Accesso illegittimo ai dati	Mitigazione Impatto (Gravità)	Mitigazione Probabilità
	Misure organizzative	Misure organizzative
Gravità: Limitato (Medio)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Probabilità: Importante (Probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Alto	+ Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro	+ Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro
	+ Informativa di 1° livello	~~– Informativa di 1° livello~~
Impatti potenziali	+ Informativa di 2° livello	~~– Informativa di 2° livello~~
+ comunicazione dei dati non autorizzata	+ Accesso alle immagini	+ Accesso alle immagini
+ diffusione dei dati non autorizzata	+ Esercizio dei diritti degli interessati	+ Esercizio dei diritti degli interessati
~~– attribuzione errata di un illecito~~	+ Tracciabilità	+ Tracciabilità
~~– non attribuzione di un illecito~~	+ Archiviazione	+ Archiviazione
	+ Minimizzazione dei dati	+ Minimizzazione dei dati
Accadimenti	+ Manutenzione	+ Manutenzione
+ malware	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento)
+ hacker	+ Amministratore di sistema	+ Amministratore di sistema
+ furto del dispositivo	+ Politica di tutela della privacy	+ Politica di tutela della privacy
~~– cancellazione involontaria~~	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
~~– cancellazione volontaria~~	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
~~– distruzione del dispositivo~~	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
Fonti	+ Lotta contro il malware	+ Lotta contro il malware
+ fonte umana esterna	+ Gestione del personale	+ Gestione del personale
+ fonte umana interna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
~~– fonte non umana~~	+ Gestione dei rischi	+ Gestione dei rischi
	Misure tecniche	Misure tecniche
	+ Criptografia	+ Criptografia
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	~~– Backup~~	~~– Backup~~

Modifiche indesiderate ai dati

Gravità: Limitato (Medio)	**Mitigazione Impatto (Gravità)**	**Mitigazione Probabilità**
Probabilità: Importante (Probabile)	**Misure organizzative**	**Misure organizzative**
Rischio: Alto	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
	+ Registro dei trattamenti	+ Registro dei trattamenti
Impatti potenziali	+ Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro	+ Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro
– comunicazione dei dati non autorizzata	– Informativa di 1° livello	– Informativa di 1° livello
– diffusione dei dati non autorizzata	– Informativa di 2° livello	– Informativa di 2° livello
+ attribuzione errata di un illecito	– Accesso alle immagini	– Accesso alle immagini
+ non attribuzione di un illecito	– Esercizio dei diritti degli interessati	– Esercizio dei diritti degli interessati
	+ Tracciabilità	+ Tracciabilità
Accadimenti	+ Archiviazione	+ Archiviazione
+ malware	+ Minimizzazione dei dati	+ Minimizzazione dei dati
+ hacker	+ Manutenzione	+ Manutenzione
+ furto del dispositivo	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento)
– cancellazione involontaria	+ Amministratore di sistema	+ Amministratore di sistema
– cancellazione volontaria	+ Politica di tutela della privacy	+ Politica di tutela della privacy
– distruzione del dispositivo	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
Fonti	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ fonte umana esterna	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
+ fonte umana interna	+ Lotta contro il malware	+ Lotta contro il malware
– fonte non umana	+ Gestione del personale	+ Gestione del personale
	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
	+ Gestione dei rischi	+ Gestione dei rischi
	Misure tecniche	**Misure tecniche**
	+ Criptografia	+ Criptografia
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	+ Backup	– Backup

Perdita dei dati	Mitigazione Impatto (Gravità)	Mitigazione Probabilità
	Misure organizzative	Misure organizzative
Gravità: Trascurabile (Lieve)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Probabilità: Massimo (Altamente probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Medio	+ Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro	+ Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro
	~~- Informativa di 1° livello~~	~~- Informativa di 1° livello~~
Impatti potenziali	~~- Informativa di 2° livello~~	~~- Informativa di 2° livello~~
~~- comunicazione dei dati non autorizzata~~	~~- Accesso alle immagini~~	~~- Accesso alle immagini~~
~~- diffusione dei dati non autorizzata~~	~~- Esercizio dei diritti degli interessati~~	~~- Esercizio dei diritti degli interessati~~
~~- attribuzione errata di un illecito~~	+ Tracciabilità	+ Tracciabilità
+ non attribuzione di un illecito	+ Archiviazione	+ Archiviazione
	+ Minimizzazione dei dati	+ Minimizzazione dei dati
Accadimenti	+ Manutenzione	+ Manutenzione
+ malware	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento)
+ hacker	+ Amministratore di sistema	+ Amministratore di sistema
+ furto del dispositivo	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ cancellazione involontaria	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
+ cancellazione volontaria	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ distruzione del dispositivo	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
Fonti	+ Lotta contro il malware	+ Lotta contro il malware
+ fonte umana esterna	+ Gestione del personale	+ Gestione del personale
+ fonte umana interna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
+ fonte non umana	+ Gestione dei rischi	+ Gestione dei rischi
	Misure tecniche	Misure tecniche
	~~- Criptografia~~	+ Criptografia
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	+ Backup	+ Backup

Mappatura dei rischi per lettura targhe

Accesso illegittimo ai dati	Mitigazione Impatto	Mitigazione Probabilità
	Misure organizzative	**Misure organizzative**
Gravità: Limitato (Medio)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Probabilità: Importante (Probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Alto	+ Informativa di 1° livello	~~- Informativa di 1° livello~~
	+ Informativa di 2° livello	~~- Informativa di 2° livello~~
Impatti potenziali	+ Accesso alle immagini	+ Accesso alle immagini
+ comunicazione dei dati non autorizzata	+ Esercizio dei diritti degli interessati	+ Esercizio dei diritti degli interessati
+ diffusione dei dati non autorizzata	+ Tracciabilità	+ Tracciabilità
~~- attribuzione errata di un illecito~~	+ Archiviazione	+ Archiviazione
~~- non attribuzione di un illecito~~	+ Minimizzazione dei dati	+ Minimizzazione dei dati
	+ Manutenzione	+ Manutenzione
Accadimenti	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del	+ Contratto con il responsabile del trattamento
+ malware	+ Amministratore di sistema	+ Amministratore di sistema
+ hacker	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ furto del dispositivo	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
~~- cancellazione involontaria~~	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
~~- cancellazione volontaria~~	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
~~- distruzione del dispositivo~~	+ Lotta contro il malware	+ Lotta contro il malware
Fonti	+ Gestione del personale	+ Gestione del personale
+ fonte umana esterna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
+ fonte umana interna	+ Gestione dei rischi	+ Gestione dei rischi
~~- fonte non umana~~	**Misure tecniche**	**Misure tecniche**
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	~~- Backup~~	~~- Backup~~

Modifiche indesiderate ai dati

Gravità: Limitato (Medio)
Probabilità: Importante (Probabile)
Rischio: Alto

Impatti potenziali
– comunicazione dei dati non autorizzata
– diffusione dei dati non autorizzata
+ attribuzione errata di un illecito
+ non attribuzione di un illecito

Accadimenti
+ malware
+ hacker
+ furto del dispositivo
– cancellazione involontaria
– cancellazione volontaria
– distruzione del dispositivo

Fonti
+ fonte umana esterna
+ fonte umana interna
– fonte non umana

Mitigazione Impatto
Misure organizzative
+ Regolamento di Videosorveglianza
+ Registro dei trattamenti
– Informativa di 1° livello
– Informativa di 2° livello
– Accesso alle immagini
– Esercizio dei diritti degli interessati
+ Tracciabilità
+ Archiviazione
+ Minimizzazione dei dati
+ Manutenzione
+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del
+ Amministratore di sistema
+ Politica di tutela della privacy
+ Gestione delle politiche di tutela della privacy
+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ Vigilanza sulla protezione dei dati
+ Lotta contro il malware
+ Gestione del personale
+ Prevenzione delle fonti di rischio
+ Gestione dei rischi
Misure tecniche
+ Controllo degli accessi logici
+ Sicurezza dell'hardware
+ Gestione postazioni
+ Sicurezza dei canali informatici
+ Controllo degli accessi fisici
+ Protezione contro fonti di rischio non umane
+ Backup

Mitigazione Probabilità
Misure organizzative
+ Regolamento di Videosorveglianza
+ Registro dei trattamenti
– Informativa di 1° livello
– Informativa di 2° livello
– Accesso alle immagini
– Esercizio dei diritti degli interessati
+ Tracciabilità
+ Archiviazione
+ Minimizzazione dei dati
+ Manutenzione
+ Contratto con il responsabile del trattamento
+ Amministratore di sistema
+ Politica di tutela della privacy
+ Gestione delle politiche di tutela della privacy
+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ Vigilanza sulla protezione dei dati
+ Lotta contro il malware
+ Gestione del personale
+ Prevenzione delle fonti di rischio
+ Gestione dei rischi
Misure tecniche
+ Controllo degli accessi logici
+ Sicurezza dell'hardware
+ Gestione postazioni
+ Sicurezza dei canali informatici
+ Controllo degli accessi fisici
+ Protezione contro fonti di rischio non umane
– Backup

Perdita dei dati	Mitigazione Impatto	Mitigazione Probabilità
	Misure organizzative	**Misure organizzative**
Gravità: Trascurabile (Lieve)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Probabilità: Massimo (Altamente probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Medio	~~– Informativa di 1° livello~~	~~– Informativa di 1° livello~~
	~~– Informativa di 2° livello~~	~~– Informativa di 2° livello~~
Impatti potenziali	~~– Accesso alle immagini~~	~~– Accesso alle immagini~~
~~– comunicazione dei dati non autorizzata~~	~~– Esercizio dei diritti degli interessati~~	~~– Esercizio dei diritti degli interessati~~
~~– diffusione dei dati non autorizzata~~	+ Tracciabilità	+ Tracciabilità
~~– attribuzione errata di un illecito~~	+ Archiviazione	+ Archiviazione
+ non attribuzione di un illecito	+ Minimizzazione dei dati	+ Minimizzazione dei dati
	+ Manutenzione	+ Manutenzione
Accadimenti	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile del	+ Contratto con il responsabile del trattamento
+ malware	+ Amministratore di sistema	+ Amministratore di sistema
+ hacker	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ furto del dispositivo	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
+ cancellazione involontaria	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ cancellazione volontaria	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
+ distruzione del dispositivo	+ Lotta contro il malware	+ Lotta contro il malware
Fonti	+ Gestione del personale	+ Gestione del personale
+ fonte umana esterna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
+ fonte umana interna	+ Gestione dei rischi	+ Gestione dei rischi
+ fonte non umana	**Misure tecniche**	**Misure tecniche**
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	+ Backup	+ Backup

Mappatura dei rischi per fototrappole

Accesso illegittimo ai dati	Mitigazione Impatto	Mitigazione Probabilità
	Misure organizzative	Misure organizzative
Gravità: Limitato (Medio)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Probabilità: Importante (Probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Alto	+ Informativa di 1° livello	~~- Informativa di 1° livello~~
	+ Informativa di 2° livello	~~- Informativa di 2° livello~~
Impatti potenziali	+ Accesso alle immagini	+ Accesso alle immagini
+ comunicazione dei dati non autorizzata	+ Esercizio dei diritti degli interessati	+ Esercizio dei diritti degli interessati
+ diffusione dei dati non autorizzata	+ Tracciabilità	+ Tracciabilità
~~- attribuzione errata di un illecito~~	+ Archiviazione	+ Archiviazione
~~- non attribuzione di un illecito~~	+ Minimizzazione dei dati	+ Minimizzazione dei dati
	+ Manutenzione	+ Manutenzione
Accadimenti	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile d	+ Contratto con il responsabile del trattamento
+ malware	+ Amministratore di sistema	+ Amministratore di sistema
+ hacker	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ furto del dispositivo	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
~~- cancellazione involontaria~~	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
~~- cancellazione volontaria~~	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
~~- distruzione del dispositivo~~	+ Lotta contro il malware	+ Lotta contro il malware
Fonti	+ Gestione del personale	+ Gestione del personale
+ fonte umana esterna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
+ fonte umana interna	+ Gestione dei rischi	+ Gestione dei rischi
~~- fonte non umana~~	Misure tecniche	Misure tecniche
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	~~- Backup~~	~~- Backup~~

Modifiche indesiderate ai dati

	Mitigazione Impatto	Mitigazione Probabilità
Gravità: Limitato (Medio)	**Misure organizzative**	**Misure organizzative**
Probabilità: Importante (Probabile)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Rischio: Alto	+ Registro dei trattamenti	+ Registro dei trattamenti
	~~– Informativa di 1° livello~~	~~– Informativa di 1° livello~~
Impatti potenziali	~~– Informativa di 2° livello~~	~~– Informativa di 2° livello~~
~~– comunicazione dei dati non autorizzata~~	~~– Accesso alle immagini~~	~~– Accesso alle immagini~~
~~– diffusione dei dati non autorizzata~~	~~– Esercizio dei diritti degli interessati~~	~~– Esercizio dei diritti degli interessati~~
+ attribuzione errata di un illecito	+ Tracciabilità	+ Tracciabilità
+ non attribuzione di un illecito	+ Archiviazione	+ Archiviazione
	+ Minimizzazione dei dati	+ Minimizzazione dei dati
Accadimenti	+ Manutenzione	+ Manutenzione
+ malware	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile d	+ Contratto con il responsabile del trattamento
+ hacker	+ Amministratore di sistema	+ Amministratore di sistema
+ furto del dispositivo	+ Politica di tutela della privacy	+ Politica di tutela della privacy
~~– cancellazione involontaria~~	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
~~– cancellazione volontaria~~	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
~~– distruzione del dispositivo~~	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
Fonti	+ Lotta contro il malware	+ Lotta contro il malware
+ fonte umana esterna	+ Gestione del personale	+ Gestione del personale
+ fonte umana interna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
~~– fonte non umana~~	+ Gestione dei rischi	+ Gestione dei rischi
	Misure tecniche	**Misure tecniche**
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	+ Backup	~~– Backup~~

Perdita dei dati	Mitigazione Impatto	Mitigazione Probabilità
	Misure organizzative	**Misure organizzative**
Gravità: Trascurabile (Lieve)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Probabilità: Massimo (Altamente probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Medio	~~- Informativa di 1° livello~~	~~- Informativa di 1° livello~~
	~~- Informativa di 2° livello~~	~~- Informativa di 2° livello~~
Impatti potenziali	~~- Accesso alle immagini~~	~~- Accesso alle immagini~~
~~- comunicazione dei dati non autorizzata~~	~~- Esercizio dei diritti degli interessati~~	~~- Esercizio dei diritti degli interessati~~
~~- diffusione dei dati non autorizzata~~	+ Tracciabilità	+ Tracciabilità
~~- attribuzione errata di un illecito~~	+ Archiviazione	+ Archiviazione
+ non attribuzione di un illecito	+ Minimizzazione dei dati	+ Minimizzazione dei dati
	+ Manutenzione	+ Manutenzione
Accadimenti	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile d	+ Contratto con il responsabile del trattamento
+ malware	+ Amministratore di sistema	+ Amministratore di sistema
+ hacker	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ furto del dispositivo	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
+ cancellazione involontaria	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ cancellazione volontaria	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
+ distruzione del dispositivo	+ Lotta contro il malware	+ Lotta contro il malware
Fonti	+ Gestione del personale	+ Gestione del personale
+ fonte umana esterna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
+ fonte umana interna	+ Gestione dei rischi	+ Gestione dei rischi
+ fonte non umana	**Misure tecniche**	**Misure tecniche**
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	+ Backup	+ Backup

Mappatura dei rischi per il sistema Rilevazione Rosso semaforico

Accesso illegittimo ai dati	Mitigazione Impatto	Mitigazione Probabilità
	Misure organizzative	Misure organizzative
Gravità: Limitato (Medio)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Probabilità: Importante (Probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Alto	+ Informativa di 1° livello	~~- Informativa di 1° livello~~
	+ Informativa di 2° livello	~~- Informativa di 2° livello~~
Impatti potenziali	+ Accesso alle immagini	+ Accesso alle immagini
+ comunicazione dei dati non autorizzata	+ Esercizio dei diritti degli interessati	+ Esercizio dei diritti degli interessati
+ diffusione dei dati non autorizzata	+ Tracciabilità	+ Tracciabilità
~~- attribuzione errata di un illecito~~	+ Archiviazione	+ Archiviazione
~~- non attribuzione di un illecito~~	+ Minimizzazione dei dati	+ Minimizzazione dei dati
	+ Manutenzione	+ Manutenzione
Accadimenti	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile d	+ Contratto con il responsabile del trattamento
+ malware	+ Amministratore di sistema	+ Amministratore di sistema
+ hacker	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ furto del dispositivo	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
~~- cancellazione involontaria~~	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
~~- cancellazione volontaria~~	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
~~- distruzione del dispositivo~~	+ Lotta contro il malware	+ Lotta contro il malware
Fonti	+ Gestione del personale	+ Gestione del personale
+ fonte umana esterna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
+ fonte umana interna	+ Gestione dei rischi	+ Gestione dei rischi
~~- fonte non umana~~	Misure tecniche	Misure tecniche
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	~~- Backup~~	~~- Backup~~

Modifiche indesiderate ai dati	Mitigazione Impatto	Mitigazione Probabilità
	Misure organizzative	Misure organizzative
Gravità: Limitato (Medio)	+ Regolamento di Videosorveglianza	+ Regolamento di Videosorveglianza
Probabilità: Importante (Probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Alto	– Informativa di 1° livello	– Informativa di 1° livello
	– Informativa di 2° livello	– Informativa di 2° livello
Impatti potenziali	– Accesso alle immagini	– Accesso alle immagini
– comunicazione dei dati non autorizzata	– Esercizio dei diritti degli interessati	– Esercizio dei diritti degli interessati
– diffusione dei dati non autorizzata	+ Tracciabilità	+ Tracciabilità
+ attribuzione errata di un illecito	+ Archiviazione	+ Archiviazione
+ non attribuzione di un illecito	+ Minimizzazione dei dati	+ Minimizzazione dei dati
	+ Manutenzione	+ Manutenzione
Accadimenti	+ Gestione dei terzi che accedono ai dati(contratto con il responsabile d	+ Contratto con il responsabile del trattamento
+ malware	+ Amministratore di sistema	+ Amministratore di sistema
+ hacker	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ furto del dispositivo	+ Gestione delle politiche di tutela della privacy	+ Gestione delle politiche di tutela della privacy
– cancellazione involontaria	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
– cancellazione volontaria	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
– distruzione del dispositivo	+ Lotta contro il malware	+ Lotta contro il malware
Fonti	+ Gestione del personale	+ Gestione del personale
+ fonte umana esterna	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
+ fonte umana interna	+ Gestione dei rischi	+ Gestione dei rischi
– fonte non umana	Misure tecniche	Misure tecniche
	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Controllo degli accessi fisici	+ Controllo degli accessi fisici
	+ Protezione contro fonti di rischio non umane	+ Protezione contro fonti di rischio non umane
	+ Backup	– Backup

Perdita dei dati

Gravità: Trascurabile (Lieve)	**Mitigazione Impatto**	**Mitigazione Probabilità**
Probabilità: Massimo (Altamente probabile)	**Misure organizzative**	**Misure organizzative**
Rischio: Medio	**+ Regolamento di Videosorveglianza**	**+ Regolamento di Videosorveglianza**
	+ Registro dei trattamenti	**+ Registro dei trattamenti**
Impatti potenziali	~~- Informativa di 1° livello~~	~~- Informativa di 1° livello~~
~~- comunicazione dei dati non autorizzata~~	~~- Informativa di 2° livello~~	~~- Informativa di 2° livello~~
~~- diffusione dei dati non autorizzata~~	~~- Accesso alle immagini~~	~~- Accesso alle immagini~~
~~- attribuzione errata di un illecito~~	~~- Esercizio dei diritti degli interessati~~	~~- Esercizio dei diritti degli interessati~~
+ non attribuzione di un illecito	**+ Tracciabilità**	**+ Tracciabilità**
	+ Archiviazione	**+ Archiviazione**
Accadimenti	**+ Minimizzazione dei dati**	**+ Minimizzazione dei dati**
+ malware	**+ Manutenzione**	**+ Manutenzione**
+ hacker	**+ Gestione dei terzi che accedono ai dati(contratto con il responsabile d**	**+ Contratto con il responsabile del trattamento**
+ furto del dispositivo	**+ Amministratore di sistema**	**+ Amministratore di sistema**
+ cancellazione involontaria	**+ Politica di tutela della privacy**	**+ Politica di tutela della privacy**
+ cancellazione volontaria	**+ Gestione delle politiche di tutela della privacy**	**+ Gestione delle politiche di tutela della privacy**
+ distruzione del dispositivo	**+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali**	**+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali**
Fonti	**+ Vigilanza sulla protezione dei dati**	**+ Vigilanza sulla protezione dei dati**
+ fonte umana esterna	**+ Lotta contro il malware**	**+ Lotta contro il malware**
+ fonte umana interna	**+ Gestione del personale**	**+ Gestione del personale**
+ fonte non umana	**+ Prevenzione delle fonti di rischio**	**+ Prevenzione delle fonti di rischio**
	+ Gestione dei rischi	**+ Gestione dei rischi**
	Misure tecniche	**Misure tecniche**
	+ Controllo degli accessi logici	**+ Controllo degli accessi logici**
	+ Sicurezza dell'hardware	**+ Sicurezza dell'hardware**
	+ Gestione postazioni	**+ Gestione postazioni**
	+ Sicurezza dei canali informatici	**+ Sicurezza dei canali informatici**
	+ Controllo degli accessi fisici	**+ Controllo degli accessi fisici**
	+ Protezione contro fonti di rischio non umane	**+ Protezione contro fonti di rischio non umane**
	+ Backup	**+ Backup**

Panoramica delle misure tecniche ed organizzative per videosorveglianza

Nella schematizzazione che segue sono riportate in forma sintetica:

- i principi fondamentali su cui si basano le misure tecniche e organizzative che sono state adottate al fine di minimizzare il rischio;
- le misure tecniche e organizzative che sono state adottate;
- i rischi che sono stati individuati.

	Principi fondamentali		
	Reg. UE 2016/69	**D.lgs. 51/2018**	Principi
1	Adeguata	Adeguata	Finalità
2	Adeguata	Adeguata	Basi legali
3	Adeguata	Adeguata	Adeguatezza dei dati
4	Adeguata	Adeguata	Esattezza dei dati
5	Adeguata	Adeguata	Periodo di conservazione
6	Adeguata	Adeguata	Informativa
7	Adeguata	Adeguata	Raccolta del consenso
8	Adeguata	Adeguata	Diritto di accesso
9	--	--	Diritto alla portabilità dei dati
10	Adeguata	Adeguata	Diritto di rettifica
11	Adeguata	Adeguata	Diritto di cancellazione
12	Adeguata	--	Diritto di limitazione
13	--	--	Diritto di opposizione
14	Adeguata	Adeguata	Responsabili del trattamento
15	Adeguata	Adeguata	Trasferimento dei dati

	Misure tecniche esistenti		
	Reg. UE 2016/69	**D.lgs. 51/2018**	Misure
1	Adeguata	Adeguata	Regolamento di Videosorveglianza
2	Adeguata	Adeguata	Registro dei trattamenti
3	---	---	Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro
4	Adeguata	Adeguata	Informativa di 1° livello
5	Adeguata	Adeguata	Informativa di 2° livello
6	Adeguata	Adeguata	Accesso alle immagini
7	Adeguata	Adeguata	Esercizio dei diritti degli interessati
8	Adeguata	Adeguata	Tracciabilità
9	Adeguata	Adeguata	Archiviazione
10	Adeguata	Adeguata	Minimizzazione dei dati
11	Adeguata	Adeguata	Manutenzione
12	Adeguata	Adeguata	Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)
13	Da implementare	Da implementare	Amministratore di sistema
14	Adeguata	Adeguata	Politica di tutela della privacy
15	Adeguata	Adeguata	Gestione delle politiche di tutela della privacy (Formazione continua)
16	Da implementare	Da implementare	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
17	Da implementare	Da implementare	Vigilanza sulla protezione dei dati
18	Adeguata	Adeguata	Lotta contro il malware
19	Adeguata	Adeguata	Gestione del personale
20	Adeguata	Adeguata	Prevenzione delle fonti di rischio
21	Da implementare	Da implementare	Gestione dei rischi
22	Adeguata	Adeguata	Crittografia
23	Adeguata	Adeguata	Controllo degli accessi logici
24	Adeguata	Adeguata	Gestione postazioni
25	Adeguata	Adeguata	Sicurezza dei canali informatici
26	Adeguata	Adeguata	Controllo degli accessi fisici
27	Adeguata	Adeguata	Sicurezza dell'hardware
28	Adeguata	Adeguata	Protezione contro fonti di rischio non umane
29	Da implementare	Da implementare	Backup

Legenda	
Adeguata	La misura è stata valutata sufficiente
Da implementare	La misura è assente o per come applicata non è ritenuta adeguata e quindi deve essere implementata
--	La misura è considerata non applicabile in relazione alle specifiche condizioni in cui viene effettuato il trattamento

Panoramica delle misure tecniche ed organizzative per lettura targhe

Nella schematizzazione che segue sono riportate in forma sintetica:

- i principi fondamentali su cui si basano le misure tecniche e organizzative che sono state adottate al fine di minimizzare il rischio;
- le misure tecniche e organizzative che sono state adottate;
- i rischi che sono stati individuati.

	Principi fondamentali		
	Reg. UE 2016/69	**D.lgs. 51/2018**	Principi
1	Adeguata	Adeguata	Finalità
2	Adeguata	Adeguata	Basi legali
3	Adeguata	Adeguata	Adeguatezza dei dati
4	Adeguata	Adeguata	Esattezza dei dati
5	Adeguata	Adeguata	Periodo di conservazione
6	Adeguata	Adeguata	Informativa
7	Adeguata	Adeguata	Raccolta del consenso
8	Adeguata	Adeguata	Diritto di accesso
9	--	--	Diritto alla portabilità dei dati
10	Adeguata	Adeguata	Diritto di rettifica
11	Adeguata	Adeguata	Diritto di cancellazione
12	Adeguata	--	Diritto di limitazione
13	--	--	Diritto di opposizione
14	Adeguata	Adeguata	Responsabili del trattamento
15	Adeguata	Adeguata	Trasferimento dei dati

	Misure tecniche esistenti		
	Reg. UE 2016/69	**D.lgs. 51/2018**	Misure
1	Adeguata	Adeguata	Presenza del trattamento di lettura targhe del Regolamento di videosorveglianza
2	Da implementare	Da implementare	Registro dei trattamenti
3	---	---	Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro
4	Adeguata	Adeguata	Informativa di 1° livello
5	Adeguata	Adeguata	Informativa di 2° livello
6	Adeguata	Adeguata	Accesso alle immagini
7	Adeguata	Adeguata	Esercizio dei diritti degli interessati
8	Adeguata	Adeguata	Tracciabilità
9	Adeguata	Adeguata	Archiviazione
10	Adeguata	Adeguata	Minimizzazione dei dati
11	Adeguata	Adeguata	Manutenzione
12	Adeguata	Adeguata	Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)
13	Da implementare	Da implementare	Amministratore di sistema
14	Adeguata	Adeguata	Politica di tutela della privacy
15	Adeguata	Adeguata	Gestione delle politiche di tutela della privacy (Formazione continua)
16	Da implementare	Da implementare	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
17	Da implementare	Da implementare	Vigilanza sulla protezione dei dati
18	Adeguata	Adeguata	Lotta contro il malware
19	Adeguata	Adeguata	Gestione del personale
20	Adeguata	Adeguata	Prevenzione delle fonti di rischio
21	Da implementare	Da implementare	Gestione dei rischi
22	Adeguata	Adeguata	Crittografia
23	Adeguata	Adeguata	Controllo degli accessi logici
24	Adeguata	Adeguata	Gestione postazioni
25	Adeguata	Adeguata	Sicurezza dei canali informatici
26	Adeguata	Adeguata	Controllo degli accessi fisici
27	Adeguata	Adeguata	Sicurezza dell'hardware
28	Adeguata	Adeguata	Protezione contro fonti di rischio non umane
29	Da implementare	Da implementare	Backup

Legenda	
Adeguata	La misura è stata valutata sufficiente
Da implementare	La misura è assente o per come applicata non è ritenuta adeguata e quindi deve essere implementata
--	La misura è considerata non applicabile in relazione alle specifiche condizioni in cui viene effettuato il trattamento

Panoramica delle misure tecniche ed organizzative per fototrappole

Nella schematizzazione che segue sono riportate in forma sintetica:

- i principi fondamentali su cui si basano le misure tecniche e organizzative che sono state adottate al fine di minimizzare il rischio;
- le misure tecniche e organizzative che sono state adottate;
- i rischi che sono stati individuati.

	Principi fondamentali		
	Reg. UE 4716/69	**D.lgs. 51/4718**	Principi
1	Adeguata	Adeguata	Finalità
2	Adeguata	Adeguata	Basi legali
3	Adeguata	Adeguata	Adeguatezza dei dati
4	Adeguata	Adeguata	Esattezza dei dati
5	Adeguata	Adeguata	Periodo di conservazione
6	Adeguata	Adeguata	Informativa
7	Adeguata	Adeguata	Raccolta del consenso
8	Adeguata	Adeguata	Diritto di accesso
9	--	--	Diritto alla portabilità dei dati
10	Adeguata	Adeguata	Diritto di rettifica
11	Adeguata	Adeguata	Diritto di cancellazione
12	Adeguata	--	Diritto di limitazione
13	--	--	Diritto di opposizione
14	Adeguata	Adeguata	Responsabili del trattamento
15	Adeguata	Adeguata	Trasferimento dei dati

	Misure tecniche esistenti		
	Reg. UE 4716/69	**D.lgs. 51/4718**	Misure
1	Adeguata	Adeguata	Presenza del trattamento delle FOTOTRAPPOLE del Regolamento di videosorveglianza
2	Da implementare	Da implementare	Registro dei trattamenti
3	---	---	Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro
4	Adeguata	Adeguata	Informativa di 1° livello
5	Adeguata	Adeguata	Informativa di 2° livello
6	Adeguata	Adeguata	Accesso alle immagini
7	Adeguata	Adeguata	Esercizio dei diritti degli interessati
8	Adeguata	Adeguata	Tracciabilità
9	Adeguata	Adeguata	Archiviazione
10	Adeguata	Adeguata	Minimizzazione dei dati
11	Adeguata	Adeguata	Manutenzione
12	Da implementare	Da implementare	Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)
13	Da implementare	Da implementare	Amministratore di sistema
14	Adeguata	Adeguata	Politica di tutela della privacy
15	Adeguata	Adeguata	Gestione delle politiche di tutela della privacy (Formazione continua)
16	Da implementare	Da implementare	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
17	Da implementare	Da implementare	Vigilanza sulla protezione dei dati
18	Adeguata	Adeguata	Lotta contro il malware
19	Adeguata	Adeguata	Gestione del personale
20	Adeguata	Adeguata	Prevenzione delle fonti di rischio
21	Da implementare	Da implementare	Gestione dei rischi
22	Adeguata	Adeguata	Crittografia
23	Adeguata	Adeguata	Controllo degli accessi logici
24	Adeguata	Adeguata	Gestione postazioni
25	Adeguata	Adeguata	Sicurezza dei canali informatici
26	Adeguata	Adeguata	Controllo degli accessi fisici
27	Adeguata	Adeguata	Sicurezza dell'hardware
28	Adeguata	Adeguata	Protezione contro fonti di rischio non umane
29	Da implementare	Da implementare	Backup

Legenda	
Adeguata	La misura è stata valutata sufficiente
Da implementare	La misura è assente o per come applicata non è ritenuta adeguata e quindi deve essere implementata
--	La misura è considerata non applicabile in relazione alle specifiche condizioni in cui viene effettuato il trattamento

Panoramica delle misure tecniche ed organizzative per Rosso Semaforico

	Principi fondamentali		
	Reg. UE 2016/69	**D.lgs. 51/2018**	Principi
1	Adeguata	Adeguata	Finalità
2	Adeguata	Adeguata	Basi legali
3	Adeguata	Adeguata	Adeguatezza dei dati
4	Adeguata	Adeguata	Esattezza dei dati
5	Adeguata	Adeguata	Periodo di conservazione
6	Adeguata	Adeguata	Informativa
7	Adeguata	Adeguata	Raccolta del consenso
8	Adeguata	Adeguata	Diritto di accesso
9	--	--	Diritto alla portabilità dei dati
10	Adeguata	Adeguata	Diritto di rettifica
11	Adeguata	Adeguata	Diritto di cancellazione
12	Adeguata	--	Diritto di limitazione
13	--	--	Diritto di opposizione
14	Adeguata	Adeguata	Responsabili del trattamento
15	Adeguata	Adeguata	Trasferimento dei dati

	Misure tecniche esistenti		
	Reg. UE 2016/69	**D.lgs. 51/2018**	Misure
1	Adeguata	Adeguata	Presenza del trattamento nel Regolamento di videosorveglianza
2	Da implementare	Da implementare	Registro dei trattamenti
3	---	---	Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro
4	Adeguata	Adeguata	Informativa di 1° livello
5	Adeguata	Adeguata	Informativa di 2° livello
6	Adeguata	Adeguata	Accesso alle immagini
7	Adeguata	Adeguata	Esercizio dei diritti degli interessati
8	Adeguata	Adeguata	Tracciabilità
9	Adeguata	Adeguata	Archiviazione
10	Adeguata	Adeguata	Minimizzazione dei dati
11	Adeguata	Adeguata	Manutenzione
12	Adeguata	Adeguata	Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)
13	Adeguata	Adeguata	Amministratore di sistema
14	Adeguata	Adeguata	Politica di tutela della privacy
15	Adeguata	Adeguata	Gestione delle politiche di tutela della privacy (Formazione continua)
16	Da implementare	Da implementare	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
17	Da implementare	Da implementare	Vigilanza sulla protezione dei dati
18	Adeguata	Adeguata	Lotta contro il malware
19	Adeguata	Adeguata	Gestione del personale
20	Adeguata	Adeguata	Prevenzione delle fonti di rischio
21	Da implementare	Da implementare	Gestione dei rischi
22	Adeguata	Adeguata	Crittografia
23	Adeguata	Adeguata	Controllo degli accessi logici
24	Adeguata	Adeguata	Gestione postazioni
25	Adeguata	Adeguata	Sicurezza dei canali informatici
26	Adeguata	Adeguata	Controllo degli accessi fisici
27	Adeguata	Adeguata	Sicurezza dell'hardware
28	Adeguata	Adeguata	Protezione contro fonti di rischio non umane
29	Adeguata	Adeguata	Backup

Legenda	
Adeguata	La misura è stata valutata sufficiente
Da implementare	La misura è assente o per come applicata non è ritenuta adeguata e quindi deve essere implementata
--	La misura è considerata non applicabile in relazione alle specifiche condizioni in cui viene effettuato il trattamento

Calcolo del rischio videosorveglianza

CALCOLO DEL RISCHIO								
		Peso	Accesso Illegittimo		Modifiche		Perdita dei	
Impatto	**Impatti potenziali**	**4**		**2**		**2**		**1**
	comunicazione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	diffusione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	attribuzione errata di un illecito	25,00%		0,00	1	1,00		0,00
	non attribuzione di un illecito	25,00%		0,00	1	1,00	1	1,00
Probabilità		**4**		**2,9**		**2,9**		**4**
	Accadimenti	**3**		**2,1**		**2,1**		**3**
	malware	25,00%	1	0,75	1	0,75	1	0,75
	hacker	25,00%	1	0,75	1	0,75	1	0,75
	furto del dispositivo	20,00%	1	0,60	1	0,60	1	0,60
	cancellazione involontaria	10,00%		0,00		0,00	1	0,30
	cancellazione volontaria	10,00%		0,00		0,00	1	0,30
	distruzione del dispositivo	10,00%		0,00		0,00	1	0,30
	Fonti	**1**		**0,8**		**0,8**		**1**
	fonte umana esterna	40,00%	1	0,40	1	0,40	1	0,40
	fonte umana interna	40,00%	1	0,40	1	0,40	1	0,40
	fonte non umana	20,00%		0,00		0,00	1	0,20
Mitigazione Impatto (Gravità)	*Valore di mitigazione**	**3,00**	**1,5**	**1,20**	**1,5**	**1,01**	**0,75**	**0,47**
	Percentuale di rischio residuo		**28,13%**	**40%**	**34,52%**	**50%**	**37,65%**	**53%**
	Misure organizzative	**2,00**	**1**	**0,76**	**1**	**0,57**	**0,5**	**0,29**
	Regolamento di Videosorveglianza	4,76%	1	0,05	1	0,05	1	0,02
	Registro dei trattamenti	4,76%	1	0,05	1	0,05	1	0,02
	Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro	4,76%	1	0,00	1	0,00	1	0,00
	Informativa di 1° livello	4,76%	1	0,05		0,00		0,00
	Informativa di 2° livello	4,76%	1	0,05		0,00		0,00
	Accesso alle immagini	4,76%	1	0,05		0,00		0,00
	Esercizio dei diritti degli interessati	4,76%	1	0,05		0,00		0,00
	Tracciabilità	4,76%	1	0,05	1	0,05	1	0,02
	Archiviazione	4,76%	1	0,05	1	0,05	1	0,02
	Minimizzazione dei dati	4,76%	1	0,05	1	0,05	1	0,02
	Manutenzione	4,76%	1	0,05	1	0,05	1	0,02
	Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento)	4,76%	1	0,02	1	0,02	1	0,01
	Amministratore di sistema	4,76%	1	0,02	1	0,02	1	0,01
	Politica di tutela della privacy	4,76%	1	0,05	1	0,05	1	0,02
	Gestione delle politiche di tutela della privacy	4,76%	1	0,05	1	0,05	1	0,02
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	4,76%	1	0,00	1	0,00	1	0,00
	Vigilanza sulla protezione dei dati	4,76%	1	0,00	1	0,00	1	0,00
	Lotta contro il malware	4,76%	1	0,05	1	0,05	1	0,02
	Gestione del personale	4,76%	1	0,05	1	0,05	1	0,02
	Prevenzione delle fonti di rischio	4,76%	1	0,05	1	0,05	1	0,02
	Gestione dei rischi	4,76%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1,00**	**0,5**	**0,44**	**0,5**	**0,44**	**0,25**	**0,19**
	Criptografia	12,50%	1	0,06	1	0,06		0,00
	Controllo degli accessi logici	12,50%	1	0,06	1	0,06	1	0,03
	Gestione postazioni	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dei canali informatici	12,50%	1	0,06	1	0,06	1	0,03
	Controllo degli accessi fisici	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dell'hardware	12,50%	1	0,06	1	0,06	1	0,03
	Protezione contro fonti di rischio non umane	12,50%	1	0,06	1	0,06	1	0,03
	Backup	12,50%		0,00	1	0,00	1	0,00
Mitigazione Probabilità	*Valore di mitigazione**	**3,00**	**2,175**	**1,60**	**2,175**	**1,46**	**3**	**2,02**
	Percentuale di rischio residuo		**32,89%**	**45%**	**37,65%**	**50%**	**34,52%**	**50%**
	Misure organizzative	**2,00**	**1,45**	**0,97**	**1,45**	**0,83**	**2**	**1,14**
	Regolamento di Videosorveglianza	4,76%	1	0,07	1	0,07	1	0,10
	Registro dei trattamenti	4,76%	1	0,07	1	0,07	1	0,10
	Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro	4,76%	1	0,00	1	0,00	1	0,00
	Informativa di 1° livello	4,76%		0,00		0,00		0,00
	Informativa di 2° livello	4,76%		0,00		0,00		0,00
	Accesso alle immagini	4,76%	1	0,07		0,00		0,00
	Esercizio dei diritti degli interessati	4,76%	1	0,07		0,00		0,00
	Tracciabilità	4,76%	1	0,07	1	0,07	1	0,10
	Archiviazione	4,76%	1	0,07	1	0,07	1	0,10
	Minimizzazione dei dati	4,76%	1	0,07	1	0,07	1	0,10
	Manutenzione	4,76%	1	0,07	1	0,07	1	0,10
	Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento)	4,76%	1	0,03	1	0,03	1	0,05
	Amministratore di sistema	4,76%	1	0,03	1	0,03	1	0,05
	Politica di tutela della privacy	4,76%	1	0,07	1	0,07	1	0,10
	Gestione delle politiche di tutela della privacy	4,76%	1	0,07	1	0,07	1	0,10
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	4,76%	1	0,00	1	0,00	1	0,00
	Vigilanza sulla protezione dei dati	4,76%	1	0,00	1	0,00	1	0,00
	Lotta contro il malware	4,76%	1	0,07	1	0,07	1	0,10
	Gestione del personale	4,76%	1	0,07	1	0,07	1	0,10
	Prevenzione delle fonti di rischio	4,76%	1	0,07	1	0,07	1	0,10
	Gestione dei rischi	4,76%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1**	**0,725**	**0,63**	**0,725**	**0,63**	**1**	**0,88**
	Criptografia	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi logici	12,50%	1	0,09	1	0,09	1	0,13
	Gestione postazioni	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dei canali informatici	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi fisici	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dell'hardware	12,50%	1	0,09	1	0,09	1	0,13
	Protezione contro fonti di rischio non umane	12,50%	1	0,09	1	0,09	1	0,13
	Backup	12,50%		0,00		0,00	1	0,00

* Viene sempre mantenuta una percentuale del 25% che non è mitigabile (viene usato come fondo scala 3 anziché 4)

Rischio originario

RISCHIO ORIGINARARIO				
AREA DI IMPATTO	MINACCIA	GRAVITA'	PROBABILITA'	RISCHIO
Riservatezza	Accesso Illegittimo	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Integrità	Modifiche indesiderate	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Disponibilità	Perdita di dati	**1,00** Trascurabile (Lieve)	**4,00** Massimo (Altamente probabile)	**4,00** Medio

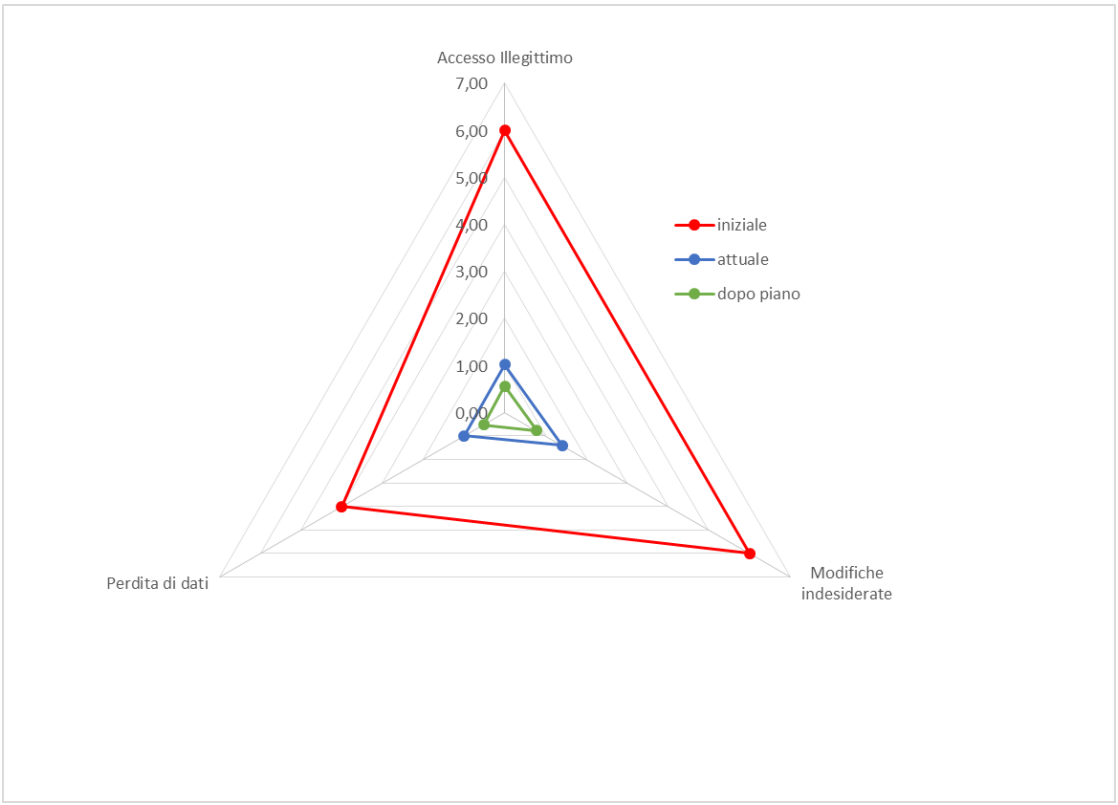
Rischio mitigato con le misure tecniche ed organizzative già adottate

RISCHIO RESIDUO ALLO STATO DELLE COSE (ATTUALE) - DOPO APPLICAZIONE MISURE DI MITIGAZIONE				
AREA DI IMPATTO	MINACCIA	GRAVITA'	PROBABILITA'	RISCHIO
Riservatezza	Accesso Illegittimo	**0,78** Trascurabile (Lieve)	**1,31** Limitato (Poco probabile)	**1,02** Basso
Integrità	Modifiche indesiderate	**0,97** Trascurabile (Lieve)	**1,45** Limitato (Poco probabile)	**1,40** Basso
Disponibilità	Perdita di dati	**0,51** Trascurabile (Lieve)	**1,93** Limitato (Poco probabile)	**1,00** Basso

Rischio mitigato con le misure tecniche ed organizzative previste dal piano di azione

RISCHIO RESIDUO DOPO L'ATTUAZIONE DELLE PIANO DI AZIONE				
AREA DI IMPATTO	MINACCIA	GRAVITA'	PROBABILITA'	RISCHIO
Riservatezza	Accesso Illegittimo	**0,56** Trascurabile (Lieve)	**0,99** Trascurabile (Improbabile)	**0,55** Basso
Integrità	Modifiche indesiderate	**0,69** Trascurabile (Lieve)	**1,13** Limitato (Poco probabile)	**0,78** Basso
Disponibilità	Perdita di dati	**0,38** Trascurabile (Lieve)	**1,38** Limitato (Poco probabile)	**0,52** Basso

Effetto delle misure tecniche ed organizzative sul rischio



	iniziale	attuale	dopo piano
Accesso Illegittimo	**6,00** Alto	**1,02** Basso	**0,55** Basso
Modifiche indesiderate	**6,00** Alto	**1,40** Basso	**0,78** Basso
Perdita di dati	**4,00** Medio	**1,00** Basso	**0,52** Basso

Calcolo del rischio lettura targhe

CALCOLO DEL RISCHIO								
		Peso	Accesso Illegittimo		Modifiche		Perdita dei dati	
Impatto	**Impatti potenziali**	**4**		**2**		**2**		**1**
	comunicazione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	diffusione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	attribuzione errata di un illecito	25,00%		0,00	1	1,00		0,00
	non attribuzione di un illecito	25,00%		0,00	1	1,00	1	1,00
Probabilità		**4**		**2,8**		**2,8**		**4**
	Accadimenti	**3**		**2,1**		**2,1**		**3**
	malware	15,00%	1	0,45	1	0,45	1	0,45
	hacker	15,00%	1	0,45	1	0,45	1	0,45
	furto del dispositivo	40,00%	1	1,20	1	1,20	1	1,20
	cancellazione involontaria	10,00%		0,00		0,00	1	0,30
	cancellazione volontaria	10,00%		0,00		0,00	1	0,30
	distruzione del dispositivo	10,00%		0,00		0,00	1	0,30
	Fonti	**1**		**0,7**		**0,7**		**1**
	fonte umana esterna	50,00%	1	0,50	1	0,50	1	0,50
	fonte umana interna	20,00%	1	0,20	1	0,20	1	0,20
	fonte non umana	30,00%		0,00		0,00	1	0,30
Mitigazione Impatto	*Valore di mitigazione**	**3,00**	**1,5**	**1,21**	**1,5**	**1,01**	**0,75**	**0,48**
	Percentuale di rischio residuo		**28%**	**39%**	**35%**	**49%**	**38%**	**53%**
	Misure organizzative	**2,00**	**1**	**0,78**	**1**	**0,58**	**0,5**	**0,29**
	Regolamento di Videosorveglianza	5,00%	1	0,05	1	0,05	1	0,03
	Registro dei trattamenti	5,00%	1	0,03	1	0,03	1	0,01
	Informativa di 1° livello	5,00%	1	0,05		0,00		0,00
	Informativa di 2° livello	5,00%	1	0,05		0,00		0,00
	Accesso alle immagini	5,00%	1	0,05		0,00		0,00
	Esercizio dei diritti degli interessati	5,00%	1	0,05		0,00		0,00
	Tracciabilità	5,00%	1	0,05	1	0,05	1	0,03
	Archiviazione	5,00%	1	0,05	1	0,05	1	0,03
	Minimizzazione dei dati	5,00%	1	0,05	1	0,05	1	0,03
	Manutenzione	5,00%	1	0,05	1	0,05	1	0,03
	Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento)	5,00%	1	0,03	1	0,03	1	0,01
	Amministratore di sistema	5,00%	1	0,03	1	0,03	1	0,01
	Politica di tutela della privacy	5,00%	1	0,05	1	0,05	1	0,03
	Gestione delle politiche di tutela della privacy	5,00%	1	0,05	1	0,05	1	0,03
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	5,00%	1	0,00	1	0,00	1	0,00
	Vigilanza sulla protezione dei dati	5,00%	1	0,00	1	0,00	1	0,00
	Lotta contro il malware	5,00%	1	0,05	1	0,05	1	0,03
	Gestione del personale	5,00%	1	0,05	1	0,05	1	0,03
	Prevenzione delle fonti di rischio	5,00%	1	0,05	1	0,05	1	0,03
	Gestione dei rischi	5,00%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1,00**	**0,5**	**0,44**	**0,5**	**0,44**	**0,25**	**0,19**
	Criptografia	12,50%	1	0,06	1	0,06		0,00
	Controllo degli accessi logici	12,50%	1	0,06	1	0,06	1	0,03
	Gestione postazioni	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dei canali informatici	12,50%	1	0,06	1	0,06	1	0,03
	Controllo degli accessi fisici	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dell'hardware	12,50%	1	0,06	1	0,06	1	0,03
	Protezione contro fonti di rischio non umane	12,50%	1	0,06	1	0,06	1	0,03
	Backup	12,50%		0,00	1	0,00	1	0,00
Mitigazione Probabilità	*Valore di mitigazione**	**3,00**	**2,1**	**1,56**	**2,1**	**1,42**	**3**	**2,03**
	Percentuale di rischio residuo		**33%**	**44%**	**38%**	**49%**	**35%**	**49%**
	Misure organizzative	**2,00**	**1,40**	**0,95**	**1,40**	**0,81**	**2,00**	**1,15**
	Regolamento di Videosorveglianza	5,00%	1	0,07	1	0,07	1	0,10
	Registro dei trattamenti	5,00%	1	0,04	1	0,04	1	0,05
	Informativa di 1° livello	5,00%		0,00		0,00		0,00
	Informativa di 2° livello	5,00%		0,00		0,00		0,00
	Accesso alle immagini	5,00%	1	0,07		0,00		0,00
	Esercizio dei diritti degli interessati	5,00%	1	0,07		0,00		0,00
	Tracciabilità	5,00%	1	0,07	1	0,07	1	0,10
	Archiviazione	5,00%	1	0,07	1	0,07	1	0,10
	Minimizzazione dei dati	5,00%	1	0,07	1	0,07	1	0,10
	Manutenzione	5,00%	1	0,07	1	0,07	1	0,10
	Contratto con il responsabile del trattamento	5,00%	1	0,04	1	0,04	1	0,05
	Amministratore di sistema	5,00%	1	0,04	1	0,04	1	0,05
	Politica di tutela della privacy	5,00%	1	0,07	1	0,07	1	0,10
	Gestione delle politiche di tutela della privacy	5,00%	1	0,07	1	0,07	1	0,10
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	5,00%	1	0,00	1	0,00	1	0,00
	Vigilanza sulla protezione dei dati	5,00%	1	0,00	1	0,00	1	0,00
	Lotta contro il malware	5,00%	1	0,07	1	0,07	1	0,10
	Gestione del personale	5,00%	1	0,07	1	0,07	1	0,10
	Prevenzione delle fonti di rischio	5,00%	1	0,07	1	0,07	1	0,10
	Gestione dei rischi	5,00%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1**	**0,7**	**0,61**	**0,7**	**0,61**	**1**	**0,88**
	Criptografia	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi logici	12,50%	1	0,09	1	0,09	1	0,13
	Gestione postazioni	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dei canali informatici	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi fisici	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dell'hardware	12,50%	1	0,09	1	0,09	1	0,13
	Protezione contro fonti di rischio non umane	12,50%	1	0,09	1	0,09	1	0,13
	Backup	12,50%		0,00		0,00	1	0,00

* Viene sempre mantenuta una percentuale del 25% che non è mitigabile (viene usato come fondo scala 3 anziché 4)

Rischio originario

RISCHIO ORIGINARARIO				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Integrità	Modifiche indesiderate	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Disponibiltà	Perdita di dati	**1,00** Trascurabile (Lieve)	**4,00** Massimo (Altamente probabile)	**4,00** Medio

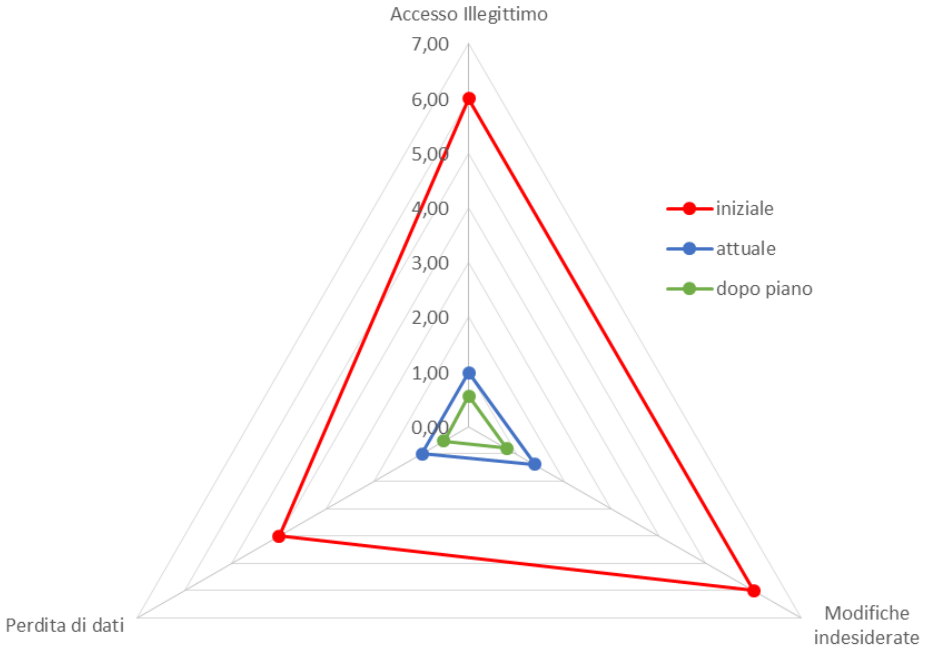
Rischio mitigato con le misure tecniche ed organizzative già adottate

RISCHIO RESIDUO ALLO STATO DELLE COSE (ATTUALE) - DOPO APPLICAZIONE MISURE DI MITIGAZIONE				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**0,76** Trascurabile (Lieve)	**1,29** Limitato (Poco probabile)	**0,99** Basso
Integrità	Modifiche indesiderate	**0,96** Trascurabile (Lieve)	**1,44** Limitato (Poco probabile)	**1,39** Basso
Disponibilità	Perdita di dati	**0,51** Trascurabile (Lieve)	**1,93** Limitato (Poco probabile)	**0,99** Basso

Rischio mitigato con le misure tecniche ed organizzative previste dal piano di azione

RISCHIO RESIDUO DOPO L'ATTUAZIONE DELLE PIANO DI AZIONE				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**0,56** Trascurabile (Lieve)	**0,99** Trascurabile (Improbabile)	**0,56** Basso
Integrità	Modifiche indesiderate	**0,70** Trascurabile (Lieve)	**1,14** Limitato (Poco probabile)	**0,80** Basso
Disponibilità	Perdita di dati	**0,38** Trascurabile (Lieve)	**1,40** Limitato (Poco probabile)	**0,53** Basso

Effetto delle misure tecniche ed organizzative sul rischio



	iniziale	attuale	dopo piano
Accesso Illegittimo	**6,00** Alto	**0,99** Basso	**0,56** Basso
Modifiche indesiderate	**6,00** Alto	**1,39** Basso	**0,80** Basso
Perdita di dati	**4,00** Medio	**0,99** Basso	**0,53** Basso

Calcolo del rischio fototrappole

CALCOLO DEL RISCHIO								
		Peso	Accesso Illegittimo		Modifiche		Perdita dei dati	
Impatto	**Impatti potenziali**	**4**		**2**		**2**		**1**
	comunicazione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	diffusione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	attribuzione errata di un illecito	25,00%		0,00	1	1,00		0,00
	non attribuzione di un illecito	25,00%		0,00	1	1,00	1	1,00
Probabilità		**4**		**2,8**		**2,8**		**4**
	Accadimenti	**3**		**2,1**		**2,1**		**3**
	malware	15,00%	1	0,45	1	0,45	1	0,45
	hacker	15,00%	1	0,45	1	0,45	1	0,45
	furto del dispositivo	40,00%	1	1,20	1	1,20	1	1,20
	cancellazione involontaria	10,00%		0,00		0,00	1	0,30
	cancellazione volontaria	10,00%		0,00		0,00	1	0,30
	distruzione del dispositivo	10,00%		0,00		0,00	1	0,30
	Fonti	**1**		**0,7**		**0,7**		**1**
	fonte umana esterna	50,00%	1	0,50	1	0,50	1	0,50
	fonte umana interna	20,00%	1	0,20	1	0,20	1	0,20
	fonte non umana	30,00%		0,00		0,00	1	0,30
Mitigazione Impatto	*Valore di mitigazione**	**3,00**	**1,5**	**1,11**	**1,5**	**0,91**	**0,75**	**0,43**
	Percentuale di rischio residuo		**28%**	**44%**	**35%**	**54%**	**38%**	**58%**
	Misure organizzative	**2,00**	**1**	**0,68**	**1**	**0,48**	**0,5**	**0,24**
	Regolamento di Videosorveglianza	5,00%	1	0,05	1	0,05	1	0,03
	Registro dei trattamenti	5,00%	1	0,03	1	0,03	1	0,01
	Informativa di 1° livello	5,00%	1	0,05		0,00		0,00
	Informativa di 2° livello	5,00%	1	0,05		0,00		0,00
	Accesso alle immagini	5,00%	1	0,05		0,00		0,00
	Esercizio dei diritti degli interessati	5,00%	1	0,05		0,00		0,00
	Tracciabilità	5,00%	1	0,05	1	0,05	1	0,03
	Archiviazione	5,00%	1	0,05	1	0,05	1	0,03
	Minimizzazione dei dati	5,00%	1	0,05	1	0,05	1	0,03
	Manutenzione	5,00%	1	0,00	1	0,00	1	0,00
	Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento)	5,00%	1	0,00	1	0,00	1	0,00
	Amministratore di sistema	5,00%	1	0,00	1	0,00	1	0,00
	Politica di tutela della privacy	5,00%	1	0,05	1	0,05	1	0,03
	Gestione delle politiche di tutela della privacy	5,00%	1	0,05	1	0,05	1	0,03
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	5,00%	1	0,00	1	0,00	1	0,00
	Vigilanza sulla protezione dei dati	5,00%	1	0,00	1	0,00	1	0,00
	Lotta contro il malware	5,00%	1	0,05	1	0,05	1	0,03
	Gestione del personale	5,00%	1	0,05	1	0,05	1	0,03
	Prevenzione delle fonti di rischio	5,00%	1	0,05	1	0,05	1	0,03
	Gestione dei rischi	5,00%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1,00**	**0,5**	**0,44**	**0,5**	**0,44**	**0,25**	**0,19**
	Criptografia	12,50%	1	0,06	1	0,06		0,00
	Controllo degli accessi logici	12,50%	1	0,06	1	0,06	1	0,03
	Gestione postazioni	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dei canali informatici	12,50%	1	0,06	1	0,06	1	0,03
	Controllo degli accessi fisici	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dell'hardware	12,50%	1	0,06	1	0,06	1	0,03
	Protezione contro fonti di rischio non umane	12,50%	1	0,06	1	0,06	1	0,03
	Backup	12,50%		0,00	1	0,00	1	0,00
Mitigazione Probabilità	*Valore di mitigazione**	**3,00**	**2,1**	**1,42**	**2,1**	**1,28**	**3**	**1,83**
	Percentuale di rischio residuo		**33%**	**49%**	**38%**	**54%**	**35%**	**54%**
	Misure organizzative	**2,00**	**1,4**	**0,81**	**1,4**	**0,67**	**2**	**0,95**
	Regolamento di Videosorveglianza	5,00%	1	0,07	1	0,07	1	0,10
	Registro dei trattamenti	5,00%	1	0,04	1	0,04	1	0,05
	Informativa di 1° livello	5,00%		0,00		0,00		0,00
	Informativa di 2° livello	5,00%		0,00		0,00		0,00
	Accesso alle immagini	5,00%	1	0,07		0,00		0,00
	Esercizio dei diritti degli interessati	5,00%	1	0,07		0,00		0,00
	Tracciabilità	5,00%	1	0,07	1	0,07	1	0,10
	Archiviazione	5,00%	1	0,07	1	0,07	1	0,10
	Minimizzazione dei dati	5,00%	1	0,07	1	0,07	1	0,10
	Manutenzione	5,00%	1	0,00	1	0,00	1	0,00
	Contratto con il responsabile del trattamento	5,00%	1	0,00	1	0,00	1	0,00
	Amministratore di sistema	5,00%	1	0,00	1	0,00	1	0,00
	Politica di tutela della privacy	5,00%	1	0,07	1	0,07	1	0,10
	Gestione delle politiche di tutela della privacy	5,00%	1	0,07	1	0,07	1	0,10
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	5,00%	1	0,00	1	0,00	1	0,00
	Vigilanza sulla protezione dei dati	5,00%	1	0,00	1	0,00	1	0,00
	Lotta contro il malware	5,00%	1	0,07	1	0,07	1	0,10
	Gestione del personale	5,00%	1	0,07	1	0,07	1	0,10
	Prevenzione delle fonti di rischio	5,00%	1	0,07	1	0,07	1	0,10
	Gestione dei rischi	5,00%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1**	**0,7**	**0,61**	**0,7**	**0,61**	**1**	**0,88**
	Criptografia	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi logici	12,50%	1	0,09	1	0,09	1	0,13
	Gestione postazioni	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dei canali informatici	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi fisici	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dell'hardware	12,50%	1	0,09	1	0,09	1	0,13
	Protezione contro fonti di rischio non umane	12,50%	1	0,09	1	0,09	1	0,13
	Backup	12,50%		0,00		0,00	1	0,00

* Viene sempre mantenuta una percentuale del 25% che non è mitigabile (viene usato come fondo scala 3 anziché 4)

Rischio originario

RISCHIO ORIGINARARIO				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Integrità	Modifiche indesiderate	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Disponibiltà	Perdita di dati	**1,00** Trascurabile (Lieve)	**4,00** Massimo (Altamente probabile)	**4,00** Medio

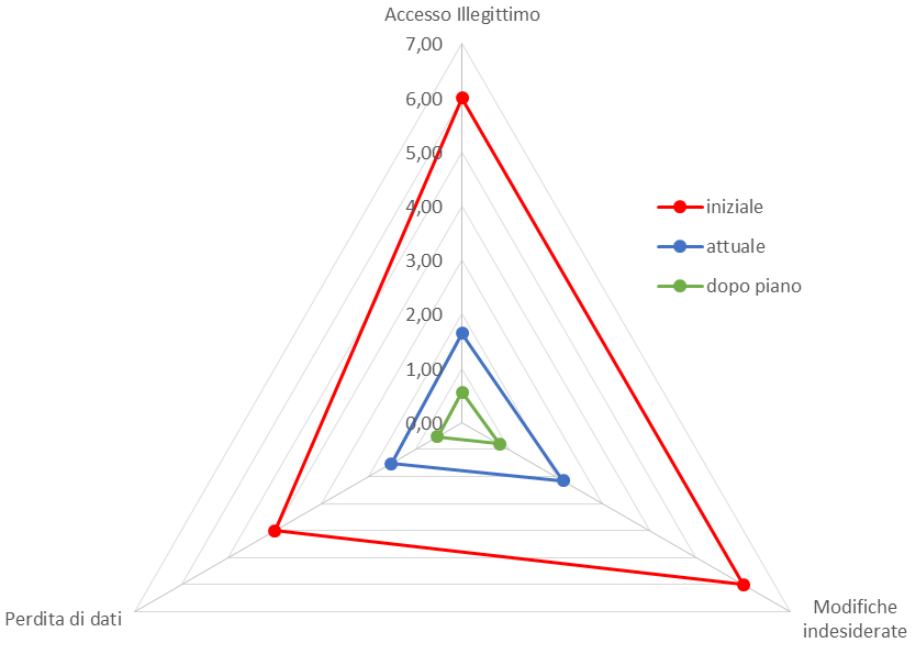
Rischio mitigato con le misure tecniche ed organizzative già adottate

RISCHIO RESIDUO ALLO STATO DELLE COSE (ATTUALE) - DOPO APPLICAZIONE MISURE DI MITIGAZIONE				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**1,00** Trascurabile (Lieve)	**1,65** Limitato (Poco probabile)	**1,65** Basso
Integrità	Modifiche indesiderate	**1,20** Limitato (Medio)	**1,80** Limitato (Poco probabile)	**2,16** Medio
Disponibilità	Perdita di dati	**0,63** Trascurabile (Lieve)	**2,40** Importante (Probabile)	**1,52** Basso

Rischio mitigato con le misure tecniche ed organizzative previste dal piano di azione

RISCHIO RESIDUO DOPO L'ATTUAZIONE DELLE PIANO DI AZIONE				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**0,56** Trascurabile (Lieve)	**0,99** Trascurabile (Improbabile)	**0,56** Basso
Integrità	Modifiche indesiderate	**0,70** Trascurabile (Lieve)	**1,14** Limitato (Poco probabile)	**0,80** Basso
Disponibilità	Perdita di dati	**0,38** Trascurabile (Lieve)	**1,40** Limitato (Poco probabile)	**0,53** Basso

Effetto delle misure tecniche ed organizzative sul rischio



	iniziale	attuale	dopo piano
Accesso Illegittimo	**6,00** Alto	**1,65** Basso	**0,56** Basso
Modifiche indesiderate	**6,00** Alto	**2,16** Medio	**0,80** Basso
Perdita di dati	**4,00** Medio	**1,52** Basso	**0,53** Basso

Calcolo del rischio Rosso Semaforico

CALCOLO DEL RISCHIO								
		Peso	Accesso Illegittimo		Modifiche		Perdita dei dati	
Impatto	**Impatti potenziali**	**4**		**2**		**2**		**1**
	comunicazione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	diffusione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	attribuzione errata di un illecito	25,00%		0,00	1	1,00		0,00
	non attribuzione di un illecito	25,00%		0,00	1	1,00	1	1,00
Probabilità		**4**		**2,8**		**2,8**		**4**
	Accadimenti	**3**		**2,1**		**2,1**		**3**
	malware	15,00%	1	0,45	1	0,45	1	0,45
	hacker	15,00%	1	0,45	1	0,45	1	0,45
	furto del dispositivo	40,00%	1	1,20	1	1,20	1	1,20
	cancellazione involontaria	10,00%		0,00		0,00	1	0,30
	cancellazione volontaria	10,00%		0,00		0,00	1	0,30
	distruzione del dispositivo	10,00%		0,00		0,00	1	0,30
	Fonti	**1**		**0,7**		**0,7**		**1**
	fonte umana esterna	50,00%	1	0,50	1	0,50	1	0,50
	fonte umana interna	20,00%	1	0,20	1	0,20	1	0,20
	fonte non umana	30,00%		0,00		0,00	1	0,30
Mitigazione Impatto	*Valore di mitigazione**	**3,00**	**1,5**	**1,21**	**1,5**	**1,08**	**0,75**	**0,51**
	Percentuale di rischio residuo		**28%**	**39%**	**35%**	**46%**	**38%**	**49%**
	Misure organizzative	**2,00**	**1**	**0,78**	**1**	**0,58**	**0,5**	**0,29**
	Regolamento di Videosorveglianza	5,00%	1	0,05	1	0,05	1	0,03
	Registro dei trattamenti	5,00%	1	0,03	1	0,03	1	0,01
	Informativa di 1° livello	5,00%	1	0,05		0,00		0,00
	Informativa di 2° livello	5,00%	1	0,05		0,00		0,00
	Accesso alle immagini	5,00%	1	0,05		0,00		0,00
	Esercizio dei diritti degli interessati	5,00%	1	0,05		0,00		0,00
	Tracciabilità	5,00%	1	0,05	1	0,05	1	0,03
	Archiviazione	5,00%	1	0,05	1	0,05	1	0,03
	Minimizzazione dei dati	5,00%	1	0,05	1	0,05	1	0,03
	Manutenzione	5,00%	1	0,05	1	0,05	1	0,03
	Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento)	5,00%	1	0,03	1	0,03	1	0,01
	Amministratore di sistema	5,00%	1	0,03	1	0,03	1	0,01
	Politica di tutela della privacy	5,00%	1	0,05	1	0,05	1	0,03
	Gestione delle politiche di tutela della privacy	5,00%	1	0,05	1	0,05	1	0,03
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	5,00%	1	0,00	1	0,00	1	0,00
	Vigilanza sulla protezione dei dati	5,00%	1	0,00	1	0,00	1	0,00
	Lotta contro il malware	5,00%	1	0,05	1	0,05	1	0,03
	Gestione del personale	5,00%	1	0,05	1	0,05	1	0,03
	Prevenzione delle fonti di rischio	5,00%	1	0,05	1	0,05	1	0,03
	Gestione dei rischi	5,00%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1,00**	**0,5**	**0,44**	**0,5**	**0,50**	**0,25**	**0,22**
	Criptografia	12,50%	1	0,06	1	0,06		0,00
	Controllo degli accessi logici	12,50%	1	0,06	1	0,06	1	0,03
	Gestione postazioni	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dei canali informatici	12,50%	1	0,06	1	0,06	1	0,03
	Controllo degli accessi fisici	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dell'hardware	12,50%	1	0,06	1	0,06	1	0,03
	Protezione contro fonti di rischio non umane	12,50%	1	0,06	1	0,06	1	0,03
	Backup	12,50%		0,00	1	0,06	1	0,03
Mitigazione Probabilità	*Valore di mitigazione**	**3,00**	**2,1**	**1,56**	**2,1**	**1,42**	**3**	**2,15**
	Percentuale di rischio residuo		**33%**	**44%**	**38%**	**49%**	**35%**	**46%**
	Misure organizzative	**2,00**	**1,4**	**0,95**	**1,4**	**0,81**	**2**	**1,15**
	Regolamento di Videosorveglianza	5,00%	1	0,07	1	0,07	1	0,10
	Registro dei trattamenti	5,00%	1	0,04	1	0,04	1	0,05
	Informativa di 1° livello	5,00%		0,00		0,00		0,00
	Informativa di 2° livello	5,00%		0,00		0,00		0,00
	Accesso alle immagini	5,00%	1	0,07		0,00		0,00
	Esercizio dei diritti degli interessati	5,00%	1	0,07		0,00		0,00
	Tracciabilità	5,00%	1	0,07	1	0,07	1	0,10
	Archiviazione	5,00%	1	0,07	1	0,07	1	0,10
	Minimizzazione dei dati	5,00%	1	0,07	1	0,07	1	0,10
	Manutenzione	5,00%	1	0,07	1	0,07	1	0,10
	Contratto con il responsabile del trattamento	5,00%	1	0,04	1	0,04	1	0,05
	Amministratore di sistema	5,00%	1	0,04	1	0,04	1	0,05
	Politica di tutela della privacy	5,00%	1	0,07	1	0,07	1	0,10
	Gestione delle politiche di tutela della privacy	5,00%	1	0,07	1	0,07	1	0,10
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	5,00%	1	0,00	1	0,00	1	0,00
	Vigilanza sulla protezione dei dati	5,00%	1	0,00	1	0,00	1	0,00
	Lotta contro il malware	5,00%	1	0,07	1	0,07	1	0,10
	Gestione del personale	5,00%	1	0,07	1	0,07	1	0,10
	Prevenzione delle fonti di rischio	5,00%	1	0,07	1	0,07	1	0,10
	Gestione dei rischi	5,00%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1**	**0,7**	**0,61**	**0,7**	**0,61**	**1**	**1,00**
	Criptografia	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi logici	12,50%	1	0,09	1	0,09	1	0,13
	Gestione postazioni	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dei canali informatici	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi fisici	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dell'hardware	12,50%	1	0,09	1	0,09	1	0,13
	Protezione contro fonti di rischio non umane	12,50%	1	0,09	1	0,09	1	0,13
	Backup	12,50%		0,00		0,00	1	0,13

* Viene sempre mantenuta una percentuale del 25% che non è mitigabile (viene usato come fondo scala 3 anziché 4)

Rischio originario

RISCHIO ORIGINARARIO				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Integrità	Modifiche indesiderate	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Disponibilità	Perdita di dati	**1,00** Trascurabile (Lieve)	**4,00** Massimo (Altamente probabile)	**4,00** Medio

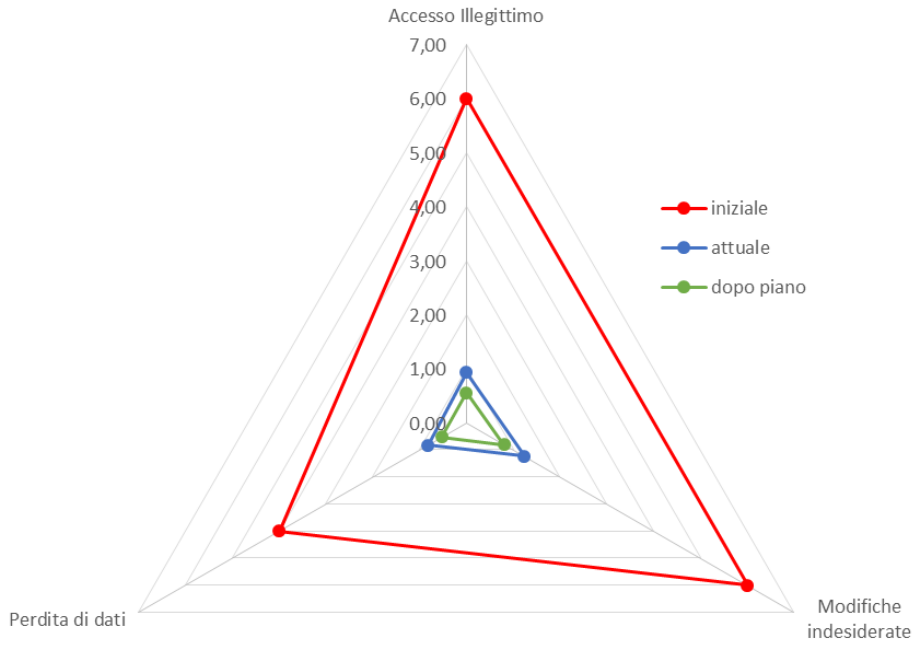
Rischio mitigato con le misure tecniche ed organizzative già adottate

RISCHIO RESIDUO ALLO STATO DELLE COSE (ATTUALE) - DOPO APPLICAZIONE MISURE DI MITIGAZIONE				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**0,74** Trascurabile (Lieve)	**1,26** Limitato (Poco probabile)	**0,93** Basso
Integrità	Modifiche indesiderate	**0,88** Trascurabile (Lieve)	**1,41** Limitato (Poco probabile)	**1,23** Basso
Disponibilità	Perdita di dati	**0,47** Trascurabile (Lieve)	**1,75** Limitato (Poco probabile)	**0,82** Basso

Rischio mitigato con le misure tecniche ed organizzative previste dal piano di azione

RISCHIO RESIDUO DOPO L'ATTUAZIONE DELLE PIANO DI AZIONE				
AREA DI IMPATTO	**MINACCIA**	**GRAVITA'**	**PROBABILITA'**	**RISCHIO**
Riservatezza	Accesso Illegittimo	**0,56** Trascurabile (Lieve)	**0,99** Trascurabile (Improbabile)	**0,56** Basso
Integrità	Modifiche indesiderate	**0,70** Trascurabile (Lieve)	**1,14** Limitato (Poco probabile)	**0,80** Basso
Disponibilità	Perdita di dati	**0,38** Trascurabile (Lieve)	**1,40** Limitato (Poco probabile)	**0,53** Basso

Effetto delle misure tecniche ed organizzative sul rischio



	iniziale	attuale	dopo piano
Accesso Illegittimo	**6,00** Alto	**0,93** Basso	**0,56** Basso
Modifiche indesiderate	**6,00** Alto	**1,23** Basso	**0,80** Basso
Perdita di dati	**4,00** Medio	**0,82** Basso	**0,53** Basso

Piano d'azione

Principi fondamentali

Rispetto ai principi fondamentali che sono stati presi in considerazione non si prevede un piano di azione per adottarne di ulteriori, in quanto quelli considerati si ritengono coerenti e adeguati al trattamento in oggetto ma migliorabili.

Misure consigliate / da pianificate

Per quanto riguarda la **VIDEOSORVEGLIANZA** le misure tecniche e organizzative attualmente implementate **POSSONO ESSERE CONSIDERATE ADEGUATE** al trattamento in oggetto, configurando un rischio di livello **BASSO**.
Si consiglia comunque di attuare il **PIANO DI AZIONE** individuato nel suo complesso al fine di mitigare ulteriormente il rischio per le persone fisiche e quello di incorrere in sanzioni dell'Autorità Garante per la protezione dei dati personali.

Per quanto riguarda l'**IMPIANTO DI LETTURA TARGHE** nel complesso le misure tecniche e organizzative attualmente implementate **POSSONO ESSERE CONSIDERATE ADEGUATE** al trattamento in oggetto, configurando un rischio di livello qualificabile come **BASSO**.
Si consiglia in ogni caso di attuare il **PIANO DI AZIONE** individuato nel suo complesso al fine di rendere il trattamento maggiormente conforme alla normativa.

Per quanto riguarda Le **FOTOTRAPPOLE** nel complesso le misure tecniche e organizzative attualmente implementate **POSSONO ESSERE CONSIDERATE ADEGUATE** al trattamento in oggetto, configurando un rischio di livello qualificabile come **BASSO**.
Si consiglia in ogni caso di attuare il **PIANO DI AZIONE** individuato nel suo complesso al fine di rendere il trattamento maggiormente conforme alla normativa.

Per quanto riguarda sistema di rilevamento **ROSSO SEMAFORICO** nel complesso le misure tecniche e organizzative attualmente implementate **POSSONO ESSERE CONSIDERATE ADEGUATE** al trattamento in oggetto, configurando un rischio di livello qualificabile come **BASSO**
Si consiglia in ogni caso di attuare il **PIANO DI AZIONE** individuato nel suo complesso al fine di rendere il trattamento maggiormente conforme alla normativa.

Si precisa inoltre che un rischio residuale BASSO è una valutazione circa i diritti e le libertà degli interessati**.**

Un rischio qualificato come BASSO non evidenzia la piena conformità al Regolamento UE 2016/679 e alle altre normative nazionali e internazionali che afferiscono alla protezione dei dati personali ma semplicemente che si valuta qualificabile come BASSO e quindi tendenzialmente come accettabile il rischio a cui si sottopongono gli interessati con i trattamenti di dati personali presi in esame in riferimento ai loro diritti e alle loro libertà. Per aumentare il grado di conformità al Regolamento UE e ridurre il rischio di incorrere in sanzioni da parte delle autorità competenti si consiglia di mettere in atto tutte le misure tecniche ed organizzative indicate nei piani di azione definiti.

Rispetto alle misure organizzative, si precisa che formano parte integrante delle misure di sicurezza, ai fini della presente, le procedure operative e il disciplinare tecnico a cui devono attenersi gli addetti interni autorizzati nell'effettuazione dei trattamenti.

Piano di azione per la videosorveglianza

Misura	Situazione in essere	Azione	Miglioramento	Data stimata	Responsabile
Amministratore di sistema	Parzialmente adeguata	Da implementare	Procedere in tempi brevi con la sottoscrizione della nomina da parte dell'Amministratore di Sistema.	Entro 6 mesi	Responsabile del servizio
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Non adeguata	Da implementare	Devono essere approvate e messe in atto una procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.	Entro 6 mesi	Responsabile del servizio
Vigilanza sulla protezione dei dati	Non adeguata	Da implementare	Si consiglia di attuare audit periodici finalizzati a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.	Entro 6 mesi	Responsabile del servizio
Gestione dei rischi	Non adeguata	Da implementare	È consigliabile definire un piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.	Entro 6 mesi	Responsabile del servizio
Responsabile del trattamento	Parzialmente adeguata	Da implementare	È necessario accertarsi che il manutentore sia stato nominato responsabile del trattamento e in caso contrario procedere alla nomina	Entro 6 mesi	
Backup	Non adeguata	Da implementare	Si consiglia di dotare il sistema di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.	Entro 6 mesi	Responsabile del servizio

Piano di azione per la lettura targhe

Misura	Situazione in essere	Azione	Miglioramento	Data stimata	Responsabile
Presenza del trattamento di lettura targhe nel Registro dei trattamenti	Parzialmente adeguata	Da implementare	Si consiglia di aggiornare il Registro dei Trattamenti dettagliando i trattamenti di videosorveglianza in funzione della tipologia di sistema di rilevazione.	Entro 6 mesi	Responsabile del servizio
Archiviazione dati per fini statistici	Parzialmente adeguata	Da Implementare	Si consiglia da archiviare i dati per fini statistici anonimizzando il dato	Entro 6 mesi	
Amministratore di sistema	Parzialmente adeguata	Da implementare	Procedere in tempi brevi con la sottoscrizione della nomina da parte dell'Amministratore di Sistema.	Entro 6 mesi	Responsabile del servizio
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Non adeguata	Da implementare	Devono essere approvate e messe in atto una procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.	Entro 6 mesi	Responsabile del servizio
Vigilanza sulla protezione dei dati	Non adeguata	Da implementare	Si consiglia di attuare audit periodici finalizzati a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.	Entro 6 mesi	Responsabile del servizio
Gestione dei rischi	Non adeguata	Da implementare	È consigliabile definire un piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.	Entro 6 mesi	Responsabile del servizio
Backup	Non adeguata	Da implementare	Si consiglia di dotare il sistema di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.	Entro 6 mesi	Responsabile del servizio

Piano di azione per le fototrappole

Misura	Situazione in essere	Azione	Miglioramento	Data stimata	Responsabile
Presenza del trattamento Fototrappole nel Registro dei Trattamenti	Parzialmente adeguata	Da implementare	Si consiglia di aggiornare il Registro dei Trattamenti dettagliando i trattamenti di videosorveglianza in funzione della tipologia di sistema di rilevazione.	Entro 6 mesi	Responsabile del servizio
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Non adeguata	Da implementare	Devono essere approvate e messe in atto una procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.	Entro 6 mesi	Responsabile del servizio
Manutenzione	Non adeguata	Da implementare	La manutenzione del sistema deve essere effettuata regolarmente e da personale qualificato per garantirne l'efficienza e sicurezza dell'impianto.	Entro 6 mesi	Responsabile del servizio
Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)	Non adeguata	Da implementare	È necessario individuare un fornitore per l'assistenza e manutenzione dei sistemi di fototrappole e regolarizzare formalmente il contratto con atto di nomina a responsabile esterno.	Entro 6 mesi	Responsabile del servizio
Amministratore di sistema	Non adeguata	Da implementare	Individuare e nominare formalmente un Amministratore di Sistema	Entro 6 mesi	Responsabile del servizio
Vigilanza sulla protezione dei dati	Non adeguata	Da implementare	Si consiglia di attuare audit periodici finalizzati a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.	Entro 6 mesi	Responsabile del servizio
Gestione dei rischi	Non adeguata	Da implementare	È consigliabile definire un piano di business continuity al fine di aumentare la capacità di	Entro 6 mesi	Responsabile del servizio

Misura	Situazione in essere	Azione	Miglioramento	Data stimata	Responsabile
			continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.		
Backup	Non adeguata	Da implementare	Si consiglia di dotare il sistema di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.	Entro 6 mesi	Responsabile del servizio

Piano di azione per il Rosso semaforico

Misura	Situazione in essere	Azione	Miglioramento	Data stimata	Responsabile
Presenza del trattamento Rilevamento Rosso Semaforico nel Registro dei Trattamenti	Parzialmente adeguata	Da implementare	Si consiglia di aggiornare il Registro dei Trattamenti dettagliando i trattamenti di videosorveglianza in funzione della tipologia di sistema di rilevazione.	Entro 6 mesi	Responsabile del servizio
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Non adeguata	Da implementare	Devono essere approvate e messe in atto una procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.	Entro 6 mesi	Responsabile del servizio
Vigilanza sulla protezione dei dati	Non adeguata	Da implementare	Si consiglia di attuare audit periodici finalizzati a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.	Entro 6 mesi	Responsabile del servizio
Presenza di un gruppo di utenti abilitato si alla gestione delle immagini live, sia alla	Parzialmente adeguata	da implementare	È opportuno limitare l'accesso soltanto al personale debitamente individuato ed autorizzato.	Entro 6 mesi	

Misura	Situazione in essere	Azione	Miglioramento	Data stimata	Responsabile
gestione delle immagini registrate e da esportare					
Gestione dei rischi	Non adeguata	Da implementare	È consigliabile definire un piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.	Entro 6 mesi	Responsabile del servizio

Rischi

Non si prevedono rischi ulteriori che potrebbero presentarsi nel tempo al variare delle condizioni.

Parere del Tecnico che ha supportato il Titolare nella valutazione, del DPO e degli interessati

Indicazioni del tecnico che ha effettuato la valutazione

Si precisa che la valutazione è stata effettuata sulla base dei dati raccolti direttamente e/o forniti dal personale e dai tecnici incaricati dall'Ente.

Tutti i dati si riferiscono a elementi funzionanti, disponibili e/o configurati sul sistema durante il periodo di osservazione.

L'analisi non ha lo scopo di valutare cause di guasti e/o malfunzionamenti.

La relazione riprende i caratteri generali dell'architettura e della configurazione del sistema, senza entrare nel dettaglio delle singole configurazioni delle componenti attive.

Dopo la valutazione del sistema di **VIDEOSORVEGLIANZA**, emerge che il trattamento dei dati (gestione di sequenze di immagini provenienti da zone pubbliche, trasmissione tramite rete sicura, memorizzazione su NVR dedicati e visualizzazione da parte del personale di Polizia Locale per l'individuazione di illeciti) rappresenta un rischio alto per i diritti e le libertà dei soggetti coinvolti. Tuttavia, riteniamo che attualmente i dispositivi e le misure tecniche ed organizzative in uso, integrate dalle procedure operative dettagliate per il trattamento, possano complessivamente mitigare questo rischio, portando il rischio residuale a un livello **BASSO**.

Nel piano d'azione allegato alla valutazione, sono identificate ulteriori misure tecniche ed organizzative che, se implementaste, adottate e applicate durante l'esercizio, contribuirebbero a ridurre ulteriormente il rischio di sanzioni da parte dell'Autorità Garante per la protezione dei dati personali, mantenendo un livello residuale basso.

Dopo la valutazione del sistema di **LETTURA TARGHE**, emerge che il trattamento dei dati (gestione di sequenze di immagini provenienti da zone pubbliche, trasmissione tramite rete sicura, memorizzazione su server dedicato alla videosorveglianza e visualizzazione da parte del personale di Polizia Locale per l'individuazione di illeciti) rappresenta un rischio alto per i diritti e le libertà dei soggetti coinvolti. Tuttavia, riteniamo che attualmente i dispositivi e le misure tecniche ed organizzative in uso, integrate dalle procedure operative dettagliate per il trattamento, possano complessivamente mitigare questo rischio, portando il rischio residuale a un livello **BASSO**.

Per quanto riguarda il sistema delle **FOTOTRAPPOLE**, a conclusione della valutazione, si rileva che, a fronte del fatto che il tipo di trattamento in sé (gestione di sequenze di immagini acquisite in zone aperte al pubblico attraverso telecamere segnalate con cartelli, scarico manuale della SD trasferimento e copia sul PC del Comandante e successiva visualizzazione delle immagini e dei relativi metadati - ora e posizione - da parte del personale in forza all'ufficio di Polizia Locale per l'individuazione di illeciti sia amministrativi che penali) rappresenta un rischio per i diritti e libertà dei soggetti interessati qualificabile come alto, si ritiene che i dispositivi e le misure tecniche ed organizzative attualmente in uso, integrate dalle procedure operative dettagliate vincolanti per gli addetti preposti al

trattamento allegate alla presente valutazione, se adottate e utilizzate durante l'esercizio, siano adeguate a mitigare il rischio riferito alle minacce di **ACCESSO ILLEGITTIMO**, di **PERDITA DI DATI** e di **MODIFICHE INDESIDERATE** portando il rischio residuale ad un livello che può essere qualificato come **BASSO**

Per quanto riguarda il sistema di **RILEVAMENTO ROSSO SEMAFORICO**, a conclusione della valutazione, si rileva che, a fronte del fatto che il tipo di trattamento in sé (gestione di sequenze di immagini acquisite in zone aperte al pubblico attraverso telecamere segnalate con cartelli, trasmissione delle immagini tramite rete informatica e sicura e relativa memorizzazione delle immagini su un server cloud e successiva visualizzazione delle immagini e dei relativi metadati - ora e posizione - da parte del personale in forza all'ufficio di Polizia Locale per l'individuazione di illeciti sia amministrativi che penali) rappresenta un rischio per i diritti e libertà dei soggetti interessati qualificabile come alto, si ritiene che i dispositivi e le misure tecniche ed organizzative attualmente in uso, integrate dalle procedure operative dettagliate vincolanti per gli addetti preposti al trattamento allegate alla presente valutazione, se adottate e utilizzate durante l'esercizio, siano adeguate a mitigare il rischio riferito alle minacce di **ACCESSO ILLEGITTIMO**, di **PERDITA DI DATI** e di **MODIFICHE INDESIDERATE** portando il rischio residuale ad un livello che può essere qualificato come **BASSO**.

Nel piano d'azione allegato alla valutazione, sono identificate ulteriori misure tecniche ed organizzative che, se implementaste, adottate e applicate durante l'esercizio, contribuirebbero a ridurre ulteriormente il rischio di sanzioni da parte dell'Autorità Garante per la protezione dei dati personali, mantenendo un livello residuale basso.

Si precisa inoltre che un rischio residuale BASSO è una valutazione circa i diritti e le libertà degli interessati. **Un rischio qualificato come BASSO non evidenzia la piena conformità al Regolamento UE 2016/679 e alle altre normative nazionali e internazionali che afferiscono alla protezione dei dati personali ma semplicemente che si valuta qualificabile come BASSO e quindi tendenzialmente come accettabile il rischio a cui si sottopongono gli interessati con i trattamenti di dati personali presi in esame in riferimento ai loro diritti e alle loro libertà**. Per aumentare il grado di conformità al Regolamento UE e ridurre il rischio di incorrere in sanzioni da parte delle autorità competenti si consiglia di mettere in atto tutte le misure tecniche ed organizzative indicate nel piano di azione.

Avendo verificato che i dispositivi in dotazione sono dotati di funzionalità tecniche adeguate a garantire, se adottate, un rischio residuale basso per i diritti e le libertà degli interessati, la possibilità di utilizzo di tali dispositivi in conformità al Regolamento UE 2016/679 e al D.Lgs. 51/2018 è subordinato all'adozione di uno stingente disciplinare operativo che definisca le modalità operative nei diversi scenari di utilizzo.

Si precisa che, come indicato nelle misure organizzative relative alla gestione del personale, la presente valutazione prevede che siano adottate le procedure operative dettagliate vincolanti per gli addetti preposti al trattamento:

- ALLEGATO 01 DPIA - DISCIPLINARE TECNICO DI ISTRUZIONE PER IL TRATTAMENTO DI VIDEOSORVEGLIANZA DI CONTESTO;
- ALLEGATO 02 DPIA - DISCIPLINARE TECNICO DI ISTRUZIONE PER IL TRATTAMENTO DI VIDEOSORVEGLIANZA DI LETTURA TARGHE;

- ALLEGATO 03 DPIA - DISCIPLINARE TECNICO DI ISTRUZIONE PER l'IMPIEGO DI SISTEMI DI VIDEOSORVEGLIANZA FOTOTRAPPOLE.
- ALLEGATO 04 DPIA - DISCIPLINARE TECNICO DI ISTRUZIONE PER l'IMPIEGO DI SISTEMI DI RILEVAMENTO ROSSO SEMAFORICO

In assenza dell'adozione di tali procedure il risultato di tale valutazione non può essere considerato attendibile.

Nome del DPO/RPD

Dott. Paolo Tiberi
Mail: dpo@comune.vittuone.mi.it

Parere del DPO/RPD

In riferimento alla DPIA del Comune di Vittuone, relativa ai sistemi di videosorveglianza, lettura targhe, foto trappole e rilevamento del rosso semaforico, lo scrivente evidenzia quanto segue:

il documento fornisce una panoramica dettagliata delle misure tecniche ed organizzative adottate e pianificate dal Titolare del Trattamento. La Valutazione dei rischi è strutturata e tiene conto degli impatti potenziali sugli interessati, delle minacce e delle fonti di rischio, nonché delle misure di mitigazione.

Tuttavia, emergono alcuni aspetti critici, che richiedono interventi concreti nel termine consigliato di 6 mesi.

In particolare è necessario in via principale:

- integrare sistemi di backup per i sistemi non ancora dotati di tale supporto. Ciò è necessario a garantire la continuità del servizio e la sicurezza dei dati, eliminando il rischio di perdita dei dati.
- Nominare un amministratore di sistema per i dati raccolti attraverso foto trappole e lettura targhe.
- Adottare una politica di gestione degli incidenti di sicurezza, istituire pertanto un registro dei data breach ed una procedura in caso di violazione dei dati;
- adottare una procedura per la distribuzione e gestione delle credenziali di accesso ai sistemi;
- limitare gli accessi alle immagini a specifici soggetti autorizzati e non a tutto il comando;
- verificare la formalizzazione di accordi scritti sulla protezione dei dati (le c.d. nomine dei responsabili del trattamento ex art. 28 del GDPR) con i fornitori che si occupano della manutenzione degli impianti.

È altresì consigliato, per i sistemi di foto trappole e lettura targhe, di motivare bene i tempi di conservazione previsti (7 giorni), verificare che i dati raccolti per finalità statistiche siano anonimizzati, ed introdurre un sistema di cancellazione automatica al fine di ridurre errori manuali e garantire il principio di minimizzazione dei dati.

Si rileva inoltre la mancanza di piani di business continuity per garantire la resilienza dei sistemi in caso di incidenti.

Alla luce delle azioni di miglioramento consigliate, il trattamento può essere considerato conforme al GDPR, a condizione che tali adempimenti siano completati entro i tempi stabiliti.

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 questi trattamenti richiedere il parere degli interessati in quanto sono trattamenti finalizzati a limitare e reprimere comportamenti illeciti. Inoltre, sono trattamenti finalizzati alla sicurezza urbana, attuati con modalità analoghe a quanto già effettuato in numerosissimi contesti simili.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento è relativo a filmati effettuati con dispostivi per l'acquisizione di immagini bidimensionali in sequenza, telecamere, per le seguenti finalità:

a) Attuazione di un sistema di sicurezza integrata ai sensi dell'art. 2 del dl 14/2017;
b) Tutela della sicurezza urbana e della sicurezza pubblica
c) Tutela degli operatori e del patrimonio comunale
d) Tutela della protezione civile e della sanità pubblica
e) Tutela della sicurezza stradale
f) Tutela ambientale e polizia amministrativa;
g) Prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali
h) Arresto in flagranza differito (Art. 10 co. 6 quater D.L. 14/2017)
i) Attuazione di atti amministrativi generali (art. 2-ter Codice privacy novellato dalla legge 205/2021)

Quali sono le responsabilità connesse al trattamento?

Il titolare è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali. Nello specifico gli obblighi sono:

- trattamento dei dati in modo lecito, corretto e trasparente nei confronti dell'interessato;

- divieto di trattamento dei dati ex art. 9 tranne nei casi di esenzione;

- informare correttamente e in maniera trasparente gli interessati;

- garantire il rispetto dei diritti degli interessati;

- adottare le misure tecniche e organizzative adeguate a garantire, sin dalla fase della progettazione e per impostazione predefinita (privacy by design e by default), la tutela dei diritti dell'interessato e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente;

- vincolo al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;

- fornire le istruzioni al responsabile del trattamento;

- tenere il registro dei trattamenti;

- fornire le istruzioni e formare il personale;

- documentare la violazione dei dati personali, notificarle al Garante e comunicarle agli interessati nei casi previsti;

- cooperare con l'autorità di controllo quando richiesto;

- redigere le valutazioni di impatto nei casi previsti;

- nominare il DPO.

Più in generale il Titolare del trattamento è soggetto alle seguenti norme di riferimento:

Norma	Titolo della fonte	Descrizione
Regolamento (UE) 2016/679	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati - RGPD)	Norma UE (regolamento) di riferimento per quanto riguarda il trattamento dei dati personali
D.Lgs. 196/2003	Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE	Norma nazionale di riferimento per quanto riguarda il trattamento dei dati personali.
Direttiva (UE) 2016/680	Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;	Norma UE (direttiva) di riferimento per quanto riguarda il trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
D.Lgs. 51/2018	Decreto Legislativo 18 maggio 2018, n. 51 – Attuazione della Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";	Norma nazionale di adattamento della direttiva UE per quanto riguarda il trattamento dei dati personali.
DPR del 15/01/2018	Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia". *L'art. 57 del D.Lgs. 196/2013 è stato abrogato a decorrere dall'8 giugno 2019, dall'art. 49, comma 2, del D.Lgs. 51/208, ma ha ripreso vigenza dal 15 giugno 2019 fino al 31 dicembre 2019. NON PIU' IN VIGORE.*	Regolamento sulle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia.
D.L. 11/2009	Decreto-Legge 23 febbraio 2009, n. 11 recante "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori." convertito con modificazioni dalla L. 23 aprile 2009, n. 38 (in G.U. 24/04/2009, n. 95)	Misure in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori.
D.L. 14/2017	Decreto-Legge 20 febbraio 2017, n. 14 recante "Disposizioni urgenti in materia di sicurezza delle città",	Disposizioni in materia di sicurezza delle città

	convertito con modificazioni dalla L. 18 aprile 2017, n. 48 (in G.U. 21/04/2017, n. 93).	
Art. 54, D.Lgs. 267/2000	Decreto Legislativo 18 agosto 2000, n. 267 Testo unico delle leggi sull'ordinamento degli enti locali.	Attribuzioni del sindaco nelle funzioni di competenza statale
DM del Ministro dell'Interno del 05/08/2008 GU 186 del 9/8/2008	Ministero dell'interno - Decreto 5 agosto 2008 Incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione. (GU Serie Generale n.186 del 09-08-2008) *Per quanto riguarda le definizioni di incolumità pubblica e sicurezza urbana ai fini di cui all'art. 54, del decreto legislativo 18 agosto 2000, n. 267, come sostituito dall'art. 6 del decreto-legge 23 maggio 2008, n. 92, convertito, con modificazioni, in legge 24 luglio 2008, n. 125.*	Incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione.
Prov. GPDP n. 1712680, 08/04/2010	Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);	Provvedimento del Garante della Protezione dei dati personali in materia di videosorveglianza
Linee Guida EDPB 3/2019	Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati (European Data Protection Board);	Linee guida dell'European Data Protection Board sul trattamento dei dati personali attraverso dispositivi video
Art.13, L. 689/1981	Legge 24 novembre 1981, n. 689 recante "Modifiche al sistema penale".	Accertamento delle violazioni amministrative
Artt. 192, 255 e 256 del D.Lgs. 152/2006	Decreto Legislativo 3 aprile 2006, n. 152 recante "Norme in materia ambientale".	Norme in materia ambientale
L. 300/1970	Legge 300/1970 (Statuto dei Lavoratori)	Norme in materia di lavoro
D.L. 139/2021	Decreto-Legge 8 ottobre 2021, n. 139 Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché' per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali, convertito con modificazioni dalla L. 3 dicembre 2021, n. 205 (in G.U. 7/12/2021, n. 291).	Per quanto riguarda la possibilità di ampliamento della base giuridica fornita alle pubbliche amministrazioni dalla modifica apportata dal D.L. 139/2021 al D.Lgs. 196/2013 con l'inserimento del comma 1-bis nell'articolo 2-ter.
Regolamento (UE) 2018/1139	Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio	Disciplina il settore dell'aviazione civile e istituisce l'Agenzia dell'Unione europea.
Regolamento (UE) 2019/947	Regolamento di esecuzione (UE) 2019/947 della Commissione del 24 maggio 2019 relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio	Disposizioni dettagliate per l'esercizio di sistemi di aeromobili senza equipaggio nonché per il personale, compresi i piloti remoti, e per le organizzazioni coinvolte in tali operazioni.
Regolamento UAS-IT - Edizione 1 del 4 gennaio 2021	Regolamento UAS-IT - Edizione 1 del 4 gennaio 2021	Disciplina degli aspetti di competenza dello Stato Membro ai sensi del Regolamento di Esecuzione (UE) 2019/947 della Commissione del 24 maggio 2019 relativo a norme e procedure per l'esercizio degli aeromobili senza equipaggio e le sue successive modificazioni.
Art. 5 comma 3-sexies D.L. 7/2015	Decreto-Legge 18 febbraio 2015, n. 7 Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché' proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo	Disciplina sulle modalità di utilizzo, da parte delle Forze di polizia, degli aeromobili a pilotaggio remoto, ai fini del controllo del territorio per

	e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione.	finalità di pubblica sicurezza, con particolare riferimento al contrasto del terrorismo e alla prevenzione dei reati di criminalità organizzata e ambientale
DM del Ministro dell'Interno del 13/06/2022 GU n.192 del 18-08-2022)	Ministero dell'Interno - Decreto 13 giugno 2022 - Modalità di utilizzo da parte delle Forze di Polizia degli aeromobili a pilotaggio remoto.	Disciplina le modalità di impiego dei sistemi di aeromobili senza equipaggio in dotazione o in uso alle Forze di polizia di cui all'art. 16 della legge 1° aprile 1981, n. 121, per le finalità di cui all'art. 5, comma 3-sexies

Ci sono standard applicabili al trattamento?

L'utilizzo dei sistemi della videosorveglianza viene attuato attraverso un corretto impiego delle applicazioni e nel rispetto dei principi applicabili al trattamento di dati personali di cui all'art. 5 dell'RGPD:

1. liceità, quale rispetto della normativa: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso, infatti, è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui i Comuni e l'ufficio di Polizia Locale sono investiti.
2. proporzionalità, con sistemi attuati con attenta valutazione: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento;
3. finalità, attuando il trattamento dei dati solo per scopi determinati ed espliciti. È consentita la videosorveglianza come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del Titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.;
4. necessità, con esclusione di uso superfluo della videosorveglianza: i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Inoltre, ai sensi del Art. 32 del RGPD, per effettuare il trattamento devono essere adottate misure tecniche ed organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio, lo stesso articolo fissa alcuni principi fondamentali. In particolare, le misure di sicurezza devono essere approntate tenendo conto dei seguenti criteri:

1. lo stato dell'arte;
2. i costi di attuazione;
3. la natura, l'oggetto, il contesto e le finalità del trattamento e
4. il rischio di varia probabilità e gravità di compressione o violazione dei diritti e delle libertà delle persone fisiche.

Le misure di sicurezza, devono essere adeguate, è imposta quindi un'obbligazione di mezzi (non di risultato), in modo che siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

Gli standard internazionali relativi alla sicurezza delle informazioni indicano che la sicurezza dei dati non riguarda solo l'aspetto informatico del trattamento, ma anche l'aspetto organizzativo, a coprire eventi quali la sottrazione o la perdita dei dati e ogni altro evento che possa non renderli disponibili e/o alterarli. Le misure di sicurezza, quindi devono garantire che:

- i dati possano essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate a farlo (e che tali persone agiscono solo nell'ambito dell'autorità che gli viene concessa);
- i dati trattati siano accurati e completi in relazione alle finalità per cui sono trattati;
- i dati rimangano accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si deve essere in grado di recuperarli e prevenire danni alle persone interessate, predisponendo un opportuno piano di continuità operativa.

La predisposizione delle misure di sicurezza richiede che il titolare sia a conoscenza dell'architettura informatica, del luogo e dei supporti con cui sono trattati i dati personali, informazione senza le quali non è possibile definire e implementare misure adeguate.

Le misure di sicurezza si dividono in due categorie: misure organizzative e misure tecniche, che, sempre secondo l'art. 32, comprendono, tra le altre:

- misura tecnica

  a) la pseudonimizzazione e la cifratura dei dati personali;

- requisiti di sicurezza

  b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

  c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

  d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Sono trattate sequenze di immagini (filmati) relative alle aree sottoposte a monitoraggio.

Il trattamento è relativo a filmati effettuati con dispostivi per l'acquisizione di immagini bidimensionali in sequenza, telecamere, per le seguenti finalità:

a) Attuazione di un sistema di sicurezza integrata ai sensi dell'art. 2 del dl 14/2017;
b) Tutela della sicurezza urbana e della sicurezza pubblica
c) Tutela degli operatori e del patrimonio comunale
d) Tutela della protezione civile e della sanità pubblica
e) Tutela della sicurezza stradale
f) Tutela ambientale e polizia amministrativa;
g) Prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali
h) Arresto in flagranza differito (Art. 10 co. 6 quater D.L. 14/2017)
i) Attuazione di atti amministrativi generali (art. 2-ter Codice privacy novellato dalla legge 205/2021)

I filmati si riferiscono a persone che transitano e sostano in queste aree.

Oltre ai dati relativi alle immagini sono trattati i relativi metadati (ora e posizione).

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

L'impianto di **videosorveglianza con telecamere fisse** con cui viene effettuato il trattamento dei dati presenta le seguenti caratteristiche salienti:

1. l'impianto di videosorveglianza è costituito da telecamere fisse (bullet) che sono state posizionate dopo attento studio e progettazione;
2. l'impianto acquisisce e memorizza in modo continuato su appositi NVR le immagini relative alle diverse zone sottoposte a monitoraggio; le immagini sono visualizzabile
3. le telecamere sono posizionate su pali difficilmente accessibili e memorizza su NVR locali posizionati negli armadietti della telecamera o NVR c/o Comando in forma crittografata e la consultazione/scarico da parte del Comando avviene attraverso linee ADSL con firewall e VPN Protetta.
4. In prossimità delle zone sottoposte a monitoraggio sono apposti cartelli di segnalazione a norma delle vigenti disposizioni normative.

Il trattamento dei dati personali deve essere effettuato con i seguenti passaggi:

1. le telecamere acquisiscono le immagini bidimensionali in sequenza riferite alle persone che transitano e sostano nelle aree poste sotto osservazione;
2. le immagini sono registrate sugli NVR posizionati negli armadietti della telecamera o NVR c/o Comando e possono essere consultate mediante collegamento su linee 4G con firewall e VPN protetta da PC ubicati all'interno di locali ad accesso controllato per il solo personale.
3. In tutti i casi in cui l'addetto autorizzato al trattamento accede agli applicativi software in dotazione per visualizzare le immagini che sono state registrate deve annotare tale evento nel registro delle visualizzazioni (identificativo dell'addetto, data e ora; periodo a cui si riferiscono i filmati da visualizzare; motivo dell'accesso) o in alternativa il sistema informatico deve generare automaticamente un file di log che registra gli accessi logici effettuati dai singoli operatori, le operazioni dagli stessi compiute sulle immagini registrate ed i relativi riferimenti temporali. Tale file deve essere protetto da cancellazione;
4. nei casi in cui l'addetto autorizzato al trattamento, durante la visualizzazione dei filmati, rilevi condotte illecite di natura amministrativa o penale, come per esempio quelle relative all'abbandono o al deposito abusivo di rifiuti sanzionato dall'art. 13 della L. 689/1981 o al compimento di atti vandalici, deve espletare l'attività di accertamento dei fatti, che comporta il download dei filmati e la compilazione di un verbale di attestazione delle operazioni, in cui deve essere annotato almeno il periodo temporale degli avvenimenti, gli eventi documentati, il luogo di installazione della telecamera;
5. le operazioni di scarico devono essere dettagliatamene registrate dall'addetto sul registro di scarico (data e ora di scarico, nome dell'addetto autorizzato al trattamento, data e ora in cui sono state riprese le immagini scaricate, fatto illecito rilevato, altre annotazioni);
6. nel caso in cui il registro di scarico sia tenuto in forma cartacea, deve essere firmato e datato dall'addetto autorizzato al trattamento che ha effettuato lo scarico e conservato presso l'ufficio di polizia locale in armadio chiuso a chiave. Nel caso in cui il registro sia tenuto in forma digitale, dopo ogni inserimento l'addetto autorizzato al trattamento deve effettuare un salvataggio in formato PDF, firmare digitalmente il file e, successivamente, salvarlo in una cartella sul server ad accesso riservato ai soli addetti autorizzati al trattamento dei dati della videosorveglianza.
7. per ogni fatto illecito rilevato, l'addetto autorizzato al trattamento deve comporre il fascicolo digitale relativo al fatto; il fascicolo deve essere composto da una relazione e dalle relative immagini utili ad avviare e svolgere il procedimento amministrativo o penale;
8. l'addetto autorizzato al trattamento che ha composto il fascicolo digitale deve assicurare che lo stesso venga conservato in una cartella criptata (della quale viene regolarmente effettuato il backup che deve essere conservato con modalità che ne garantiscano la sicurezza e minimizzino il rischio di perdita dei dati e di accesso da parte di soggetti non autorizzati);

9. nel caso il fascicolo debba essere trasmesso ad altri organi di Polizia o all'autorità giudiziaria, la trasmissione deve avvenire con modalità sicure;
10. tutte le operazioni effettuate devono essere segnate sull'apposito registro di scarico con le modalità descritte in precedenza e annotate su relativo verbale di attestazione delle operazioni che deve seguire il fascicolo;
11. quando il procedimento è di competenza esterna all'ufficio di Polizia locale e quindi il fascicolo deve essere trasmesso ad altro organo di Polizia o all'autorità giudiziaria, l'addetto autorizzato al trattamento deve assicurare che il fascicolo venga cancellato in modo irreversibile da tutti i dispositivi in cui è stato eventualmente memorizzato (compreso i supporti di backup) durante le operazioni di sua competenza;

Quali sono le risorse di supporto ai dati?

Le risorse che ospitano i dati oggetto del trattamento sono:

- gli hard disk del server di memorizzazione dei filmati;
- gli eventuali i supporti di backup;
- la rete utilizzata per scaricare/visualizzare i dati dalle telecamere;
- gli NVR e/o i server collocati presso il comune o le console e i totem utilizzati per visualizzare e scaricare i dati.
- il PC/server utilizzato per la visualizzazione delle immagini e per comporre il fascicolo e un eventuale cartella del server dove viene conservato il registro degli scarichi;
- i supporti di memorizzazione utilizzati per conservare i dati in caso di accertamento di un illecito.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità di utilizzo dell'impianto di videosorveglianza sono relative alle funzioni istituzionali demandate ai Sindaci ed ai Comuni:

a. dal decreto-legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 "disposizioni urgenti in materia di sicurezza delle città";

b. dal D.Lgs. 18 agosto 2000, n. 267, dal D.P.R. 24 luglio 1977, n. 616;

c. dalla legge sull'ordinamento della Polizia Locale 7 marzo 1986, n. 65 nonché dallo Statuto Comunale e dai Regolamenti Comunali vigenti;

d. dal D.lgs. 152/2006 del Codice dell'ambiente;

e possono essere così riassunte:

a. attivare misure di prevenzione e sicurezza sul territorio Comunale;

b. proteggere l'incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e sicurezza pubblica, la prevenzione, accertamento o repressione dei reati o esecuzione di sanzioni penali a norma del D.Lgs. 51/2018;

c. le attività di rilevazione, prevenzione e controllo delle infrazioni, nel quadro delle competenze attribuite dalla legge;

d. l'acquisizione di fonti di prove in ambito delle attività di polizia amministrativa;

e. controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;

f. monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;

g. verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;

Si precisa che tra le finalità di utilizzo dell'impianto non sono comprese quelle dell'art. 4 dello Statuto dei lavoratori (legge 300 del 20 maggio 1970) relative al controllo a distanza dell'attività dei lavoratori per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento è la lettera e) dell'art. 6 del Reg. (UE) 2016/679: "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;".

In particolare, il riferimento normativo è di individuare nell'art. 54 del D.Lgs. 267/2000 relativo alle Attribuzioni del sindaco nelle funzioni di competenza statale e alle disposizioni contenute nell'articolo 6, commi 7 e 8, del decreto-legge 23 febbraio 2009, secondo le quali i comuni possono utilizzare i sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per finalità di tutela della sicurezza urbana e la conservazione dei dati, delle informazioni e delle immagini raccolte è limitata ai sette giorni successivi alla rilevazione avvenuta a mezzo di tali sistemi, fatte salve speciali esigenze di ulteriore conservazione,

Valutazione: Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati) in quanto il trattamento delle immagini acquisite attraverso l'utilizzo del sistema di videosorveglianza è effettuato solo in aree in cui non risulta possibile il ricorso a strumenti e sistemi di controllo alternativi anche per limitatezza delle risorse umane che possono essere adibite all'effettuazione dei controlli necessari a garantire la sicurezza urbana,

Si consideri che le disposizioni legislative in materia di sicurezza attribuiscono ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidate ad essi dalla legge in materia di sicurezza e di polizia giudiziaria.

Inoltre, al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento.

Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le Forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.

Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di video sorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.

L'effetto deterrente costituito dalla presenza di un sistema di videosorveglianza ha fatto registrare evidenze significative.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

I dati sono intrinsecamente esatti e aggiornati in quanto acquisiti in modo automatico attraverso dispostivi (telecamere) per l'acquisizione di immagini bidimensionali in sequenza, i quali vengono scaricati dal server solo nel caso venga rilevata una condotta illecita.

Nel suddetto caso viene espletata l'attività di accertamento dell'illecito facendo uso dei filmati scaricati dal sistema.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Per le immagini che non documentano un fatto illecito il periodo massimo di conservazione di dati è di 7 giorni.

Nel momento in cui se ne presenti l'esigenza, a fronte di una segnalazione e/o fronte della constatazione di un atto vandalico o altro fatto illecito un addetto autorizzato al trattamento visiona i firmati registrati.

Nel caso vengano individuate immagini che documentano visivamente un fatto illecito la sequenza delle immagini a esso riferito vengono scaricate in un'apposita cartella protetta del Server.

Per quanto riguarda i filmati che vengono scaricati per effettuare l'accertamento delle violazioni il periodo di conservazione è limitato alle esigenze di conservazione dei filmati ai fini della composizione del fascicolo utile alla definizione del procedimento.

Il fascicolo viene consegnato con modalità sicure al soggetto che avvia e svolge il procedimento amministrativo o penale; al termine di tale operazione i documenti sono cancellati in modo irreversibile.

Per quanto riguarda la conservazione dei numeri di targa sia acquisti dall'addetto autorizzato mediate osservazione diretta sia attraverso sistemi automatici come gli OCR (Optical Character Recognition) il periodo di conservazione può essere esteso fino ad un massimo di 180 giorni per finalità di indagine, mediante un ulteriore atto in applicazione del comma 1-bis, art. 2-ter, dando notizia di tale termine nell'informativa completa ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito internet comunale e prevedendo tale estensione nel Regolamento comunale sulla videosorveglianza.

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

1) In conformità alle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati (European Data Protection Board) e a quanto disposto degli artt. 13-14 dell'RGDP è adottato un approccio scalare, attraverso una combinazione di metodi al fine di assicurare la trasparenza che prevede:

a. una segnaletica di avvertimento nei pressi delle telecamere (primo livello);

b. un'informativa di dettaglio fornita attraverso una pagina internet dove sono disponibili le informazioni di secondo livello (secondo livello).

2) Le informazioni di primo livello sono posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi).

Non è rivelata l'ubicazione della telecamera ma l'interessato è messo nelle condizioni di stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

Le informazioni fornite esplicitano: le finalità del trattamento, l'identità del Titolare del trattamento e l'esistenza dei diritti dell'interessato, la base giuridica del trattamento e i recapiti del responsabile della protezione dei dati, la trasmissione dati a terzi, il periodo di conservazione oltre all'indicazione della pagina internet dove sono disponibili le informazioni di secondo livello.

Per la segnaletica di avvertimento è utilizzato un modello conforme al fac-simile riportato sulle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati (European Data Protection Board)

In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, sono installati più cartelli.

La segnaletica di avvertimento nei pressi delle telecamere (primo livello) nello specifico:

- è collocata prima del raggio di azione della telecamera, nelle sue immediate vicinanze;
- ha un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza è attivo in orario notturno;
- ingloba un simbolo stilizzato di esplicita e immediata comprensione.

Per quanto riguarda gli eventuali dispositivi mobili di registrazione l'informativa di primo livello può essere resa anche in forma verbale (dashcam) o attraverso l'apposizione di un pittogramma esplicativo sull'auto di servizio dotata di dashcam.

3) Le informazioni di secondo livello sono facilmente accessibili per l'interessato e messe a disposizione attraverso la pagina internet indicata sull'informativa di primo livello e contengono tutti gli elementi obbligatori a norma dell'art. 13 dell'RGPD e dell'art.10 D.Lgs. 51/2018.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Non è richiesto il consenso degli interessati: la base giuridica del trattamento è la lettera e) dell'art. 6 del Reg. (UE) 2016/679, secondo cui "il trattamento è necessario per l'esecuzione

di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;".

Nel caso in cui la violazione rilevata comporti una sanzione penale, non è richiesto il consenso, in quanto il titolo giuridico del trattamento è il comma 1 dell'art.5 del D.Lgs. 51/2018.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto di accesso?

DIRETTIVA POLIZIA – D.Lgs. 51/2018

L'esercizio del **diritto di accesso è disciplinato dall'art. 11 del D.lgs. 18 maggio 2018, n. 51**, nel caso in cui sia svolto dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali (incluse salvaguardia e prevenzione di minacce alla sicurezza pubblica).

L'art. 11 del D.lgs. 18 maggio 2018, n. 51, fa sì che l'interessato possa ottenere da parte del Titolare la conferma dell'esistenza di una delle seguenti informazioni: le finalità e il titolo giuridico del trattamento, le categorie di dati personali trattati, i destinatari o le categorie di destinatari a cui i dati personali sono stati comunicati, il periodo di conservazione dei dati personali o, se non è possibile, i criteri per determinare tale periodo, la rettifica o la cancellazione dei dati personali, la limitazione del trattamento dei dati personali che lo riguardano, il diritto di proporre reclamo al Garante, con i relativi dati di contatto e la comunicazione dei dati personali oggetto del trattamento e di tutte le informazioni disponibili sulla loro origine.

L'esercizio del diritto di accesso può essere ritardato, limitato o escluso nella misura e per un tempo necessario e proporzionato ai diritti fondamentali e agli legittimi interessi della persona fisica interessata, al fine di non compromettere il buon esito dell'attività di prevenzione, indagine, accertamento, perseguimento di reati, l'esecuzione di sanzioni penali, nonché l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza, tutela della sicurezza pubblica, sicurezza nazionale, diritti e libertà altrui.

Il Titolare del trattamento informa l'Interessato in forma scritta di ogni rifiuto o limitazione dell'accesso e dei relativi motivi, nonché del diritto di proporre reclamo dinanzi al Garante, informato dei fatti, o di proporre ricorso giurisdizionale.

REGOLAMENTO GENERALE SULLA PROTEZIOE DEI DATI PERSONALI - Regolamento UE 2016/679

Ai sensi dell'**art. 15 del Regolamento UE 2016/679** l'interessato ha il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in caso di risposta affermativa, può ottenere l'accesso alle seguenti informazioni: le finalità del trattamento, le categorie di dati personali in questione, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali, quando possibile il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo, l'esistenza del diritto alla rettifica o la cancellazione

dei dati personali, la limitazione e l'opposizione al trattamento, il diritto di proporre reclamo a un'autorità di controllo, le informazioni disponibili sull'origine dei dati, l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato, inoltre, qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, si possono richiedere le garanzie previste dall'art. 46.

Il Titolare del trattamento fornisce una copia dei dati personali, anonimizzando ogni dato che consenta l'identificazione di ulteriori soggetti non richiedenti, e, nel caso in cui siano richieste più copie, il Titolare del trattamento può addebitare un contributo spese basato sui costi amministrativi.

L'autorità potrà negare l'accesso nel caso in cui l'interessato abbia avanzato una richiesta che possa compromettere indagini, inchieste, procedimenti ufficiali o giudiziali, accertamento, perseguimento di reati ed esecuzione di sanzioni penali, quando sia infondata e/o ripetitiva, quando abbia ad oggetto informazioni di cui è già in possesso o a cui non può accedere, oppure quando l'interessato non può essere identificato.

L'eventuale rifiuto o limitazione dell'accesso saranno motivati e comunicati all'istante, conformemente con l'art. 12, par. 3, del Regolamento UE 2016/679. Al contrario, in caso di valutazione positiva della fondatezza della richiesta, il Titolare, provvederà per iscritto ad informare l'interessato istante di quali dati personali è in possesso.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto alla portabilità dei dati?

DIRETTIVA POLIZIA – D.Lgs. 51/2018

Non è previsto il diritto alla portabilità per i trattamenti effettuati ai sensi del D.Lgs. 51/2018.

REGOLAMENTO GENERALE SULLA PROTEZIOE DEI DATI PERSONALI - Regolamento UE 2016/679

Non è possibile per l'interessato esercitare il diritto alla portabilità ai sensi dell'art. 20 del Reg. (UE) 2016/679 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 diritto di rettifica?

DIRETTIVA POLIZIA – D.Lgs. 51/2018

Il diritto alla **rettifica dei dati è previsto dagli artt. 12 e 14 D.lgs. 18 maggio 2018, n. 51**.

Ai sensi di questi due articoli, l'interessato ha il diritto di ottenere dal Titolare del trattamento, senza ingiustificato ritardo, la rettifica dei dati a patto che: non compromettano il buon esito dell'attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, nonché' l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza, tutelino la sicurezza pubblica, nazionale, diritti e libertà altrui.

Il diritto in questione si ritiene possa essere esercitato solamente nel caso in cui debba essere segnalata l'erroneità o la clonazione di una targa comparsa nelle videoriprese, che comporti la necessaria rettificazione della black list di Polizia. Ogni mezzo di trasporto che viaggia sotto l'occhio della videocamera è, attraverso un sistema di riconoscimento targhe, identificato, controllato e, se necessario, inserito nella black list di Polizia. Essa contiene una serie di dati funzionali alla sicurezza urbana, quindi, deve essere modificata nel caso in cui vi sia difformità tra una targa comparsa nelle immagini o rilevata e il veicolo realmente transitato. Ciò potrebbe accadere nell'ipotesi in cui la targa sia stata collegata ad un veicolo per errore oppure risulti clonata; quindi, non identifica il mezzo effettivamente ripreso.

REGOLAMENTO GENERALE SULLA PROTEZIOE DEI DATI PERSONALI - Regolamento UE 2016/679

Per gli effetti dell'**art. 16 del Regolamento UE 2016/679** l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

Valutazione: Accettabile

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

DIRETTIVA POLIZIA – D.Lgs. 51/2018

Il diritto alla cancellazione dei dati può avvenire ai sensi ai sensi dell'**art. 12 del D.lgs. 18 maggio 2018, n. 51**.

Sulla base a tale articolo l'interessato ha il diritto di ottenere la cancellazione dei dati personali quando il trattamento si pone in contrasto con i principi dettati dall'art. 3, con la liceità del trattamento sancita dall'art. 5 e con le disposizioni dell'art. 7.

In luogo della cancellazione, il Titolare, dispone la limitazione del trattamento quando l'esattezza dei dati, contestata dall'interessato, non può essere accertata o se i dati devono essere conservati a fini probatori.

Ai sensi dell'art. 16 della Direttiva UE 2016/680, il Titolare del trattamento può rifiutare la cancellazione quando potrebbe essere idonea a compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o esecuzione di sanzioni penali, oppure quando è necessario proteggere la sicurezza pubblica, la sicurezza nazionale, i diritti e le libertà altrui.

REGOLAMENTO GENERALE SULLA PROTEZIOE DEI DATI PERSONALI - Regolamento UE 2016/679

L'**art. 17 del Regolamento 2016/679** dispone che il diritto alla cancellazione possa essere esercitato quando non sono più necessari rispetto alle finalità per le quali sono stati raccolti

o altrimenti trattati, se non sussiste altro fondamento giuridico per il trattamento oppure alcun motivo legittimo prevalente per procedere al trattamento, nei casi previsti dall'art. 21, par. 2, oppure se i dati personali sono stati trattati illecitamente, se devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'UE o dello Stato membro cui è soggetto il Titolare del trattamento, se sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art. 8, par. 1.

Ciò, a patto che essi non servano per l'esercizio del diritto alla libertà di espressione e di informazione, per l'adempimento di un obbligo legale che richieda il Trattamento previsto dall'UE o dallo Stato membro cui è soggetto il Titolare del trattamento, per l'esecuzione di un compito svolto nel pubblico interesse, per l'esercizio di pubblici poteri di cui è investito il Titolare del trattamento, per motivi di interesse pubblico, per l'accertamento o/e per l'esercizio o la difesa di un diritto in sede giudiziaria.

Ricevuta la richiesta, se conforme, il Titolare procede alla cancellazione dandone comunicazione scritta all'istante. In caso contrario, ovvero nell'eventualità che non si possa procedere alla cancellazione dei dati, del rifiuto della richiesta e della motivazione a supporto verrà data notizia all'istante.

Nel caso in cui pervenga una richiesta di cancellazione inerente dati che devono essere conservati in forza di ulteriori normative, il Titolare del trattamento può riservarsi di non procedere alla cancellazione dandone sempre comunicazione al richiedente.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto di limitazione?

DIRETTIVA POLIZIA – D.Lgs. 51/2018

Ai sensi dell'**art. 12 del D.lgs. 18 maggio 2018, n. 51** l'interessato ha il diritto di ottenere la cancellazione dei dati personali quando il trattamento si pone in contrasto con i principi dettati dall'art. 3, con la liceità del trattamento sancita dall'art. 5 e con le disposizioni dell'art. 7.

Nel caso l'esattezza dei dati, contestata dall'interessato, non può essere accertata o se i dati devono essere conservati a fini probatori, **in luogo della cancellazione, il Titolare, dispone la limitazione** del trattamento.

REGOLAMENTO GENERALE SULLA PROTEZIOE DEI DATI PERSONALI - Regolamento UE 2016/679

Ai sensi dell'**art. 18 del Regolamento UE 2016/679** l'interessato ha il diritto di ottenere la limitazione del trattamento dei dati personali che lo riguardano quando:

1) contesta l'esattezza dei dati personali (nei limiti della durata di conservazione);
2) il trattamento è illecito;
3) l'interessato ha necessità di utilizzare i suoi dati per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria benché il titolare non abbia più bisogno di questi dati; infine, quando l'interessato si oppone al trattamento dei suoi dati.

Nel caso si verificano le condizioni per l'esercizio del diritto di limitazione, l'interessato deve presentare istanza per l'esercizio dei diritti dell'interessato al Responsabile della Protezione dei dati del Comune, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sul sito istituzionale del Comune nella sezione "Privacy") ovvero al Designato o direttamente al Titolare.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto di opposizione?

DIRETTIVA POLIZIA – D.Lgs. 51/2018

Non è previsto il diritto all'opposizione per i trattamenti effettuati ai sensi del D.Lgs. 51/2018.

REGOLAMENTO GENERALE SULLA PROTEZIOE DEI DATI PERSONALI - Regolamento UE 2016/679

Ai sensi dell'**art. 21 del Regolamento UE 2016/679** l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettera e), compresa la profilazione sulla base di tali disposizioni.

Il titolare del trattamento deve astenersi dal trattare ulteriormente i dati personali salvo sia in grado di dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Nel caso si verificano le condizioni per l'esercizio del diritto di opposizione, l'interessato deve presentare istanza per l'esercizio dei diritti dell'interessato al Responsabile della Protezione dei dati del Comune, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sul sito istituzionale del Comune nella sezione "Privacy") ovvero al Designato o direttamente al Titolare.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti?

PROCEDURA PER L'ESERCIZIO DEI DIRITTI

Il Titolare assicura agli interessati l'esercizio dei propri diritti, in particolare quelli

- di accesso ai dati personali conservati presso il Titolare;
- di opporsi al trattamento dei dati;
- di chiedere una copia dei dati;
- di chiedere la cancellazione dei dati;
- di ottenere il blocco dei dati trattati in violazione di legge.

Come già riportato, gli interessati possono esercitare in rari casi il diritto di aggiornamento, rettificazione in considerazione della natura intrinseca dei dati raccolti in tempo reale e riguardanti un fatto obiettivo.

La risposta ad una richiesta di accesso può comprendere eventuali dati riferiti a terzi nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato ed ove non siano lesi i diritti e le libertà altrui.

Gli interessati possono trasmettere le proprie richieste mediante la compilazione di un modulo predisposto dal Titolare e messo a disposizione sul sito internet istituzionale, da inviarsi via e-mail all'indirizzo indicato nel modulo.

Il Titolare fornisce all'interessato le informazioni richieste senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Se necessario, tale termine può essere prorogato di due mesi ove la richiesta sia trasmessa senza l 'utilizzo del modulo sopra indicato e ciò abbia reso necessari tempi lunghi di lavorazione della domanda o in conseguenza della complessità o del numero delle richieste. Il Titolare informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Ove il Titolare di trattamento, non fosse in grado di identificare i dati personali oggetto della richiesta dell'interessato o non avesse certezza del fatto che i dati oggetto della richiesta sono propri dell'interessato, ne informa l'interessato, chiedendo di fornire ulteriori informazioni. In tali casi, il termine per la risposta decorre dal momento della risposta dell'interessato alla richiesta di integrazione.

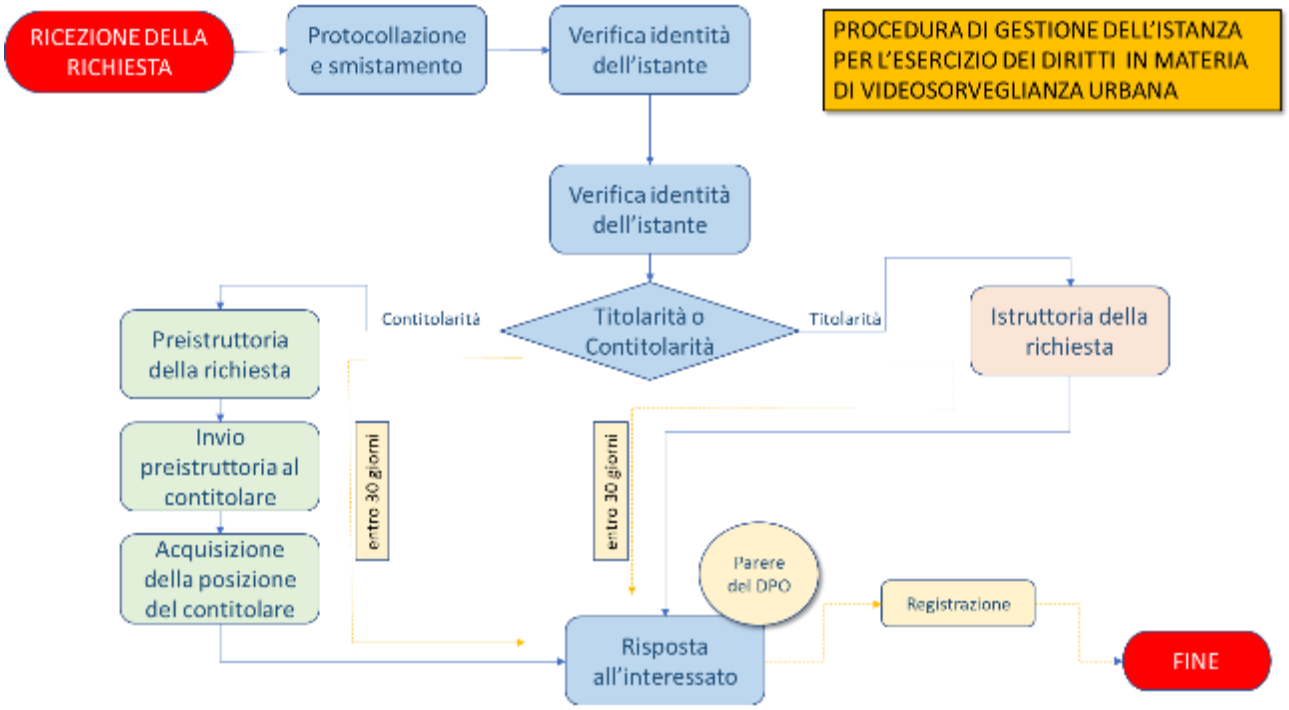
L'interessato ha il diritto di presentare reclamo al Data Protection Officer designato e/o al Garante per la Tutela dei dati personali.

TABELLA SINTESI ESERCIZIO DIRITTI CONCRETAMENTE ESERCITABILI

Diritto	Regolamento UE 2016/679	D.Lgs. 51/2018 (Direttiva di Polizia)
Diritto di accesso	Esercitabile	Esercitabile
Diritto alla portabilità	Non esercitabile	Non esercitabile
Diritto di rettifica	Rari casi	Rari casi (lettura targhe)
Diritti di cancellazione (oblio)	Esercitabile	Esercitabile in determinate condizioni
Diritto di limitazione	Esercitabile	In sostituzione della cancellazione in determinati casi
Diritto di opposizione	Esercitabile	Non esercitabile

FASI DEL PROCESSO DI GESTIONE DELLA RICHIESA DI ESERCIZIO DEI DIRITTI

Il flusso di gestione di una richiesta di esercizio dei diritti è di seguito rappresentato:



Valutazione: Accettabile

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

Nel caso si riveli necessario fare ricorso ad un responsabile esterno del trattamento, gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati con atto di nomina (contratto) ai sensi e per gli effetti del art. 28 Reg. UE 2016/679.

Ogni contratto definisce la tipologia del trattamento e dati trattati e con riferimento agli obblighi inerenti al mandato del Responsabile lo impegna ad adottare tutte le misure necessarie all'attuazione delle disposizioni di legge contenute nel Reg.to Europeo 2016/679. Il contratto definisce dello specifico:

- i termini relativi al trattamento dei dati;

- le modalità di comunicazione di dati;

- le misure per garantire l'affidabilità del trattamento e la non divulgazione dei dati;

- le misure tecniche ed organizzative adeguate a garantire la sicurezza del trattamento;

- la catena delle responsabilità;

- i diritti degli interessati;

- le modalità di gestione delle eventuali violazione dei dati personali;

- la collaborazione richiesta per l'effettuazione della valutazione d'impatto sulla protezione dei dati personali;

- le modalità operative per la cancellazione o la restituzione dei dati;

- il diritto di audit del titolare nei confronti del responsabile;

- le modalità per un eventuale trasferimento di dati personali da parte del Responsabile nei confronti di un sub-responsabile;

- l'impegno all'adozione e rispetto di codici di condotta e certificazioni;

- una serie di condizioni generali.

Nello specifico non è stato nominato alcun Responsabile del trattamento, in quanto tutte le operazioni relative al trattamento dei dati sono effettuate da personale interno.

Valutazione: Accettabile

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

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

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate sistema di videosorveglianza

	Misura	Situazione in essere	Azione di miglioramento
1	**Regolamento di Videosorveglianza**	**Adeguata**	**Nessuna**
		È presente il regolamento di videosorveglianza.	
2	**Registro dei trattamenti**	**Adeguata**	**Nessuna**
		Il trattamento di videosorveglianza è stato inserito nel registro dei trattamenti.	
3	**Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro**	**Non applicabile**	**Nessuna**
		Non vengono effettuate riprese in aree dove vengono effettuate le prestazioni di lavoro dei dipendenti comunali	
4	**Informativa di 1° livello**	**Adeguata**	**Nessuna**
		Sono presenti cartelli di segnalazione visibili prima che i soggetti entrino nel raggio di ripresa della telecamera.	
5	**Informativa di 2° livello**	**Adeguata**	**Nessuna**
		È presente un'informativa aggiornata di 2° livello ed è pubblicata sul sito dell'Ente.	
6	**Accesso alle immagini**	**Adeguata**	**Nessuna**
		È stata adottata una policy per la gestione delle richieste di accesso alle immagini completa di modulistica per le richieste di accesso alle immagini.	
7	**Esercizio dei diritti degli interessati**	**Adeguata**	**Nessuna**
		E' stata definita una procedura per la gestione dell'esercizio dei diritti degli interessati.	
8	**Tracciabilità**	**Adeguata**	**Nessuna**
		Sono presenti file di log che documentano le operazioni di visualizzazione delle immagini e le operazioni di scarico delle immagini relative a fatti illeciti. Conservazione file di log per 6 mesi.	
9	**Archiviazione**	**Parzialmente adeguata**	**Nessuna**
		I tempi di archiviazione sono limitati a 7 giorni e trascorso tale periodo i dati sono cancellati in modo irreversibile (fatta eccezione per le immagini oggetto di indagine e nei casi previsti per le targhe rilevate dagli appositi varchi.	Integrare sistema di backup
10	**Minimizzazione dei dati**	**Adeguata**	**Nessuna**
		I dati trattati si limitano ai dati strettamente necessari al perseguimento delle finalità dichiarate.	
11	**Manutenzione**	**Adeguata**	**Nessuna**
		E' presente un servizio NOC H24 che tiene sotto controllo tutti i dispositivi in rete e invia segnalazioni in caso di anomalia. La manutenzione è affidata a società esterna.	
12	**Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)**	**Adeguata**	**Implementare**
		E' stato sottoscritto contratto e relativo atto di nomina nei confronti della ditta SKP Tecnology che svolge l'attività di manutenzione del sistema.	

	Misura	Situazione in essere	Azione di miglioramento
13	**Amministratore di sistema**	**Parzialmente adeguata**	**Implementare**
		In corso la preparazione documentale per l'affidamento della funzione di Amministratore di sistema alla ditta SKP Tecnology	Procedere con la sottoscrizione dell'atto di nomina ad AdS prima dell'avvio del sistema.
14	**Politica di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio di Polizia locale ha implementato un'organizzazione interna pienamente idonea a garantire l'adeguatezza della protezione dei dati personali sono state adeguatamente formalizzate le nomine e le istruzioni dei i soggetti interni autorizzati ad effettuare il trattamento dei dati personali.	
15	**Gestione delle politiche di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio di polizia pianifica periodicamente sessioni formative per il personale del Comando. Ultima sessione formativa effettuata nel 2° semestre 2023.	
16	**Gestire gli incidenti di sicurezza e le violazioni dei dati personali**	**Non Adeguata**	**Implementare**
		Non sono presenti procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.	Devono essere approvate e messe in atto una procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.
17	**Vigilanza sulla protezione dei dati**	**Non Adeguata**	**Implementare**
		Non risultano pianificati interventi di audit periodici atti a rilevare la corretta applicazione delle misure di sicurezza per la protezione dei dati personali.	Si consiglia di attuare audit periodici finalizzati a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.
18	**Lotta contro il malware**	**Adeguata**	**Nessuna**
		Sui pc client sono presenti ed aggiornati gli applicativi di security (antivirus anti-malware ransomware etc..) e i sistemi operativi sono aggiornati.	
19	**Gestione del personale**	**Adeguata**	**Nessuna**
		Tutte le attività che interessano la videosorveglianza sono demandate al responsabile del Comando mediante decreto sindacale.	
20	**Prevenzione delle fonti di rischio**	**Adeguata**	**Nessuna**
		Seppur non presente in origine contestualmente alla valutazione d'impatto è stata condotta una puntuale valutazione dei rischi sul trattamento di videosorveglianza	
21	**Gestione dei rischi**	**Non adeguata**	**Da implementare**
		Non è ancora stato definito un adeguato piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.	È consigliabile definire un piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.
22	**Crittografia**	**Adeguata**	**Nessuna**
		Il sistema gestisce le immagini e le registra in formato proprietario con crittografia. Tutte le comunicazioni sono crittografate e i database sono protetti.	
23	**Controllo degli accessi logici**	**Adeguata**	**Nessuna**

	Misura	Situazione in essere	Azione di miglioramento
		Sono utilizzate password complesse (almeno otto caratteri almeno una maiuscola un numero ed un carattere speciale) con un sistema che impone di cambiarle ogni 90 giorni.	
24	**Gestione postazioni**	**Adeguata**	**Nessuna**
		Le postazioni o altri dispositivi, che consentono di accedere alle immagini, sono dotati di adeguati controlli logici di accesso per garantire che le persone che li utilizzano siano solo quelle autorizzate formalmente a effettuare i trattamenti di videosorveglianza.	
25	**Sicurezza dei canali informatici**	**Adeguata**	**Nessuna**
		il collegamento tramite ADSL si realizza attraverso VPN protetta, firewall e credenziali personali di accesso alla piattaforma HIKCONNET	
26	**Controllo degli accessi fisici**	**Adeguata**	**Nessuna**
		Per le telecamere, antenne, router, switch, cabine stradali, ecc…, sono state adottate adeguate misure per limitare l'accesso a tali risorse alle sole persone formalmente autorizzate.	
27	**Sicurezza dell'hardware**	**Adeguata**	**Nessuna**
		Installazione in quota per telecamere e antenne ed in locali chiusi a chiave per server e/o NVR.	
28	**Protezione contro fonti di rischio non umane**	**Adeguata**	**Nessuna**
		Installazione eseguita con criterio per evitare che l'acqua danneggi l'hardware.	
29	**Backup**	**Non adeguata**	**Da implementare**
		Il sistema non è dotato di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.	Si consiglia di dotare il sistema di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.
30	**Prefettura**	**Non applicabile**	**Nessuna**
31	**Forze di Polizia**	**Non applicabile**	**Nessuna**
32	**Telecamere di privati integrate**	**Non applicabile**	**Nessuna**
33	**Visualizzazione di privati**	**Non applicabile**	**Nessuna**

Misure esistenti o pianificate sistema di lettura targhe

	Misura	Situazione in essere	Azione di miglioramento
1	**Presenza del trattamento di lettura targhe del Regolamento di videosorveglianza**	**Adeguata**	**Nessuna**
		il regolamento rimanda a disciplinare specifico	
2	**Registro dei trattamenti**	**Parzialmente adeguata**	**Nessuna**
		Sul registro dei trattamenti è presente il trattamento generico di videosorveglianza.	Si consiglia di aggiornare il Registro dei Trattamenti dettagliando i trattamenti di videosorveglianza in funzione della tipologia di sistema di rilevazione.
3	**Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro**	**Non applicabile**	**Nessuna**
4	**Informativa di 1° livello**	**Adeguata**	**Nessuna**
		Sono presenti i cartelli di segnalazione videosorveglianza e sono visibili prima che i soggetti entrino nel raggio di ripresa della telecamera.	
5	**Informativa di 2° livello**	**Adeguata**	**Nessuna**
		È presente un'informativa aggiornata di 2° livello ed è pubblicata sul sito dell'Ente.	
6	**Accesso alle immagini**	**Adeguata**	**Nessuna**
		È stata adottata una policy per la gestione delle richieste di accesso alle immagini completa di modulistica per le richieste di accesso alle immagini.	
7	**Esercizio dei diritti degli interessati**	**Adeguata**	**Nessuna**
		E' stata definita una procedura per la gestione degli esercizi degli interessati.	
8	**Tracciabilità**	**Adeguata**	**Nessuna**
		Sono presenti file di log che documentano le operazioni di visualizzazione delle immagini e le operazioni di scarico delle immagini relative a fatti illeciti. Conservazione per 6 mesi.	
9	**Archiviazione**	**Parzialmente adeguata**	**Nessuna**
		I tempi di archiviazione sono limitati a 7 giorni e trascorso tale periodo i dati sono cancellati in modo irreversibile (fatta eccezione per le immagini oggetto di indagine e nei casi previsti per le targhe rilevate dagli appositi varchi.	Se i dati sono archiviati per fini statistici per un periodo superiore a 7 giorni, è ncessario anonimizzare i dati. è necessario inoltre motivare adeguatamente la necessità di archivare le immagini per un periodo 7 giorni, in conformità con il principi di minimazzazione dei dati
10	**Minimizzazione dei dati**	**Adeguata**	**Nessuna**
		I dati trattati si limitano ai dati strettamente necessari al perseguimento delle finalità dichiarate.	
11	**Manutenzione**	**Adeguata**	**Nessuna**
		La manutenzione del sistema è stata affidata ad una ditta esterna e viene effettuata regolarmente.	
12	**Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)**	**Adeguata**	**Implementare**
		E' stato sottoscritto contratto e relativo atto di nomina nei confronti della ditta SKP Tecnology che svolge l'attività di manutenzione del sistema.	

	Misura	Situazione in essere	Azione di miglioramento
13	**Amministratore di sistema**	**Parzialmente adeguata**	**Implementare**
		In corso la preparazione documentale per l'affidamento della funzione di Amministratore di sistema alla ditta SKP Tecnology	Completare in tempi brevi la predisposizione e sottoscrizione
14	**Politica di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio di Polizia locale ha implementato un'organizzazione interna pienamente idonea a garantire l'adeguatezza della protezione dei dati personali sono state adeguatamente formalizzate le nomine e le istruzioni dei i soggetti interni autorizzati ad effettuare il trattamento dei dati personali.	
15	**Gestione delle politiche di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio di polizia pianifica periodicamente sessioni formative per il personale del Comando. Ultima sessione formativa effettuata nel 2° semestre 2023.	
16	**Gestire gli incidenti di sicurezza e le violazioni dei dati personali**	**Non Adeguata**	**Implementare**
		Non sono presenti procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.	Devono essere approvate e messe in atto una procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.
17	**Vigilanza sulla protezione dei dati**	**Non Adeguata**	**Implementare**
		Non risultano pianificati interventi di audit periodici atti a rilevare la corretta applicazione delle misure di sicurezza per la protezione dei dati personali.	Si consiglia di attuare audit periodici finalizzati a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.
18	**Lotta contro il malware**	**Adeguata**	**Nessuna**
		Sui pc client sono presenti ed aggiornati gli applicativi di security (antivirus anti-malware ransomware etc..) e i sistemi operativi sono aggiornati.	
19	**Gestione del personale**	**Adeguata**	**Nessuna**
		Tutte le attività che interessano la videosorveglianza sono demandate al responsabile del Comando mediante decreto sindacale.	
20	**Prevenzione delle fonti di rischio**	**Adeguata**	**Nessuna**
		Seppur non presente in origine contestualmente alla valutazione d'impatto è stata condotta una puntuale valutazione dei rischi sul trattamento di videosorveglianza	
21	**Gestione dei rischi**	**Non adeguata**	**Da implementare**
		Non è ancora stato definito un adeguato piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.	È consigliabile definire un piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.
22	**Crittografia**	**Adeguata**	**Nessuna**
		Il sistema gestisce le immagini e le registra in formato proprietario con crittografia. Tutte le comunicazioni sono crittografate e i database sono protetti.	

	Misura	Situazione in essere	Azione di miglioramento
23	**Controllo degli accessi logici**	**Adeguata**	**Nessuna**
		Sono utilizzate password complesse (almeno otto caratteri almeno una maiuscola un numero ed un carattere speciale) con un sistema che impone di cambiarle ogni 90 giorni.	
24	**Gestione postazioni**	**Adeguata**	**Nessuna**
		Le postazioni o altri dispositivi, che consentono di accedere alle immagini, sono dotati di adeguati controlli logici di accesso per garantire che le persone che li utilizzano siano solo quelle autorizzate formalmente a effettuare i trattamenti di videosorveglianza.	
25	**Sicurezza dei canali informatici**	**Adeguata**	**Nessuna**
		il collegamento tramite ADSL si realizza attraverso VPN protetta, firewall e credenziali personali di accesso alla piattaforma HIKCONNET	
26	**Controllo degli accessi fisici**	**Adeguata**	**Nessuna**
		Per le telecamere, antenne, router, switch, cabine stradali, ecc…., sono state adottate adeguate misure per limitare l'accesso a tale risorse alle sole persone formalmente autorizzate.	
27	**Sicurezza dell'hardware**	**Adeguata**	**Nessuna**
		Per gli NVR e per le altre risorse di rete (telecamere, antenne, router, switch, cabine stradali, ecc…) sono state adottate adeguate misure per limitare l'accesso a tale risorse alle sole persone formalmente autorizzate.	
28	**Protezione contro fonti di rischio non umane**	**Adeguata**	**Nessuna**
		Installazione eseguita con criterio per evitare che l'acqua danneggi l'hardware.	
29	**Backup**	**Non adeguata**	**Da implementare**
		Il sistema non è dotato di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.	Si consiglia di dotare il sistema di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.
30	**Prefettura**	**Non Applicabile**	**Nessuna**
31	**Forze di Polizia**	**Non Applicabile**	**Nessuna**

Misure esistenti o pianificate per le fototrappole

	Misura	Situazione in essere	Azione di miglioramento
1	**Presenza del trattamento Fototrappole nel Regolamento di videosorveglianza**	**Adeguata**	**Nessuna**
		È presente il regolamento di videosorveglianza	
2	**Registro dei trattamenti**	**Parzialmente adeguata**	**Nessuna**
		Sul registro dei trattamenti è presente il trattamento generico di videosorveglianza.	Si consiglia di aggiornare il Registro dei Trattamenti dettagliando i trattamenti di videosorveglianza in funzione della tipologia di sistema di rilevazione.
3	**Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro**	**Non applicabile**	**Nessuna**

	Misura	Situazione in essere	Azione di miglioramento
4	**Informativa di 1° livello**	**Adeguata**	**Nessuna**
		Sono presenti i cartelli di segnalazione videosorveglianza e sono visibili prima che i soggetti entrino nel raggio di ripresa della telecamera.	
5	**Informativa di 2° livello**	**Adeguata**	**Nessuna**
		È presente un'informativa aggiornata di 2° livello ed è pubblicata sul sito dell'Ente.	
6	**Accesso alle immagini**	**Adeguata**	**Nessuna**
		È stata adottata una policy per la gestione delle richieste di accesso alle immagini completa di modulistica per le richieste di accesso alle immagini.	
7	**Esercizio dei diritti degli interessati**	**Adeguata**	**Nessuna**
		E' stata definita una procedura per la gestione degli esercizi degli interessati.	
8	**Tracciabilità**	**Adeguata**	**Nessuna**
		Sono adottati appositi registri che documentano le operazioni di visualizzazione delle immagini e le operazioni di scarico delle immagini relative a fatti illeciti.	
9	**Archiviazione**	**Parzialmente Adeguata**	**Nessuna**
		I tempi di archiviazione sono limitati a 7 giorni e trascorso tale periodo i dati sono cancellati manualmente.	è consigliabile prevedere un sistema di cancellazione automatica delle immagini al fine di ridurre la possibilità di errore. Inoltre è necessario motivare adeguatamente la necessità di archivare le immagini per un periodo 7 giorni, in conformità con il principi di minimazzazione dei dati
10	**Minimizzazione dei dati**	**Adeguata**	**Nessuna**
		I dati trattati si limitano ai dati strettamente necessari al perseguimento delle finalità dichiarate.	
11	**Manutenzione**	**Non adeguata**	**Implementare**
		La manutenzione non viene fatta periodicamente.	La manutenzione deve essere schedulata e fatta periodicamente.
12	**Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)**	Non applicabile	**Nessuna**
13	**Amministratore di sistema**	**Non adeguata**	**Implementare**
		Non è presente un Amministratore di Sistema	E' necessario individuare e nominare un Amministratore di Sistema
14	**Politica di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio di Polizia locale ha implementato un'organizzazione interna pienamente idonea a garantire l'adeguatezza della protezione dei dati personali sono state adeguatamente formalizzate le nomine e le istruzioni dei i soggetti interni autorizzati ad effettuare il trattamento dei dati personali.	
15	**Gestione delle politiche di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio di polizia pianifica periodicamente sessioni formative per il personale del Comando. Ultima sessione formativa effettuata nel 2° semestre 2023.	

	Misura	Situazione in essere	Azione di miglioramento
16	**Gestire gli incidenti di sicurezza e le violazioni dei dati personali**	**Non Adeguata**	**Implementare**
		Non sono presenti procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.	Devono essere approvate e messe in atto una procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.
17	**Vigilanza sulla protezione dei dati**	**Non Adeguata**	**Implementare**
		Non risultano pianificati interventi di audit periodici atti a rilevare la corretta applicazione delle misure di sicurezza per la protezione dei dati personali.	Si consiglia di attuare audit periodici finalizzati a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.
18	**Lotta contro il malware**	**Adeguata**	**Nessuna**
		Antivirus di windows attivo e aggiornamenti periodici attivi su PC dove vengono scaricati i filmati.	
19	**Gestione del personale**	**Adeguata**	**Nessuna**
		Tutte le attività che interessano la vds sono demandate al responsabile del Comando mediante decreto sindacale.	
20	**Prevenzione delle fonti di rischio**	**Adeguata**	**Nessuna**
		Seppur non presente in origine contestualmente alla valutazione d'impatto è stata condotta una puntuale valutazione dei rischi sul trattamento di videosorveglianza	
21	**Gestione dei rischi**	**Non adeguata**	**Da implementare**
		Non è ancora stato definito un adeguato piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.	È consigliabile definire un piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.
22	**Crittografia**	**Adeguata**	**Nessuna**
		Il sistema gestisce le immagini e le registra in formato proprietario con crittografia.	
23	**Controllo degli accessi logici**	**Adeguata**	**Nessuna**
		Sono utilizzate password complesse con un sistema che impone di cambiarle ogni 3 mesi.	
24	**Gestione postazioni**	**Adeguata**	**Nessuna**
		Le postazioni o altri dispositivi, che consentono di accedere alle immagini, sono dotati di adeguati controlli logici di accesso per garantire che le persone che li utilizzano siano solo quelle autorizzate formalmente a effettuare i trattamenti di videosorveglianza.	
25	**Sicurezza dei canali informatici**	**Parzialmente Adeguata**	**Implementare**
		IL trasferimento avviene manualmente.	
26	**Controllo degli accessi fisici**	**Adeguata**	**Nessuna**
		Per il server e per le altre risorse di rete (telecamere, antenne, router, switch, cabine stradali, ecc…) sono state adottate adeguate misure per limitare l'accesso a tale risorse alle sole persone formalmente autorizzate.	

	Misura	Situazione in essere	Azione di miglioramento
27	**Sicurezza dell'hardware**	**Adeguata**	**Nessuna**
		Installazione in armadi protetti accessibili al solo personale autorizzato.	
28	**Protezione contro fonti di rischio non umane**	**Adeguata**	**Nessuna**
		Installazione eseguita con criterio per evitare che l'acqua danneggi l'hardware.	
29	**Backup**	**Non adeguata**	**Da implementare**
		Il sistema non è dotato di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.	Si consiglia di dotare il sistema di una soluzione per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.

Misure esistenti o pianificate sistema di rilevazione Rosso semaforico

	Misura	Situazione in essere	Azione di miglioramento
1	**Presenza del trattamento Rosso Semaforico nel Regolamento di videosorveglianza**	**Adeguata**	**Nessuna**
		È presente il regolamento di videosorveglianza	
2	**Registro dei trattamenti**	**Parzialmente adeguata**	**Nessuna**
		Sul registro dei trattamenti è presente il trattamento generico di videosorveglianza.	Si consiglia di aggiornare il Registro dei Trattamenti dettagliando i trattamenti di videosorveglianza in funzione della tipologia di sistema di rilevazione.
3	**Accordo sindacale/Autorizzazione Ispettorato Provinciale del Lavoro**	**Non applicabile**	**Nessuna**
4	**Informativa di 1° livello**	**Adeguata**	**Nessuna**
		Sono presenti i cartelli di segnalazione videosorveglianza e sono visibili prima che i soggetti entrino nel raggio di ripresa della telecamera.	
5	**Informativa di 2° livello**	**Adeguata**	**Nessuna**
		È presente un'informativa aggiornata di 2° livello ed è pubblicata sul sito dell'Ente.	
6	**Accesso alle immagini**	**Parzialmente adeguata**	**Nessuna**
		E' stata adottata una policy per la gestione delle richieste di accesso alle immagini.	Accertarsi che possano accedere alle immagini soltanto i soggetti debitamente individuati ed autorizzati
7	**Esercizio dei diritti degli interessati**	**Adeguata**	**Nessuna**
		E' stata definita una procedura per la gestione degli esercizi degli interessati.	
8	**Tracciabilità**	**Adeguata**	**Nessuna**
		Sono presenti file di log che documentano le operazioni svolte sul sistema	
9	**Archiviazione**	**Parzialmente adeguata**	**Nessuna**
		I tempi di archiviazione sono limitati a 7 giorni e trascorso tale periodo i dati sono cancellati in modo irreversibile (fatta eccezione per le immagini oggetto di indagine e nei casi previsti per le targhe rilevate dagli appositi varchi.	è necessario motivare adeguatamente la necessità di archivare le immagini per un periodo 7 giorni, in conformità con il principi di minimazzazione dei dati

	Misura	Situazione in essere	Azione di miglioramento
10	**Minimizzazione dei dati**	**Adeguata**	**Nessuna**
		I dati trattati si limitano ai dati strettamente necessari al perseguimento delle finalità dichiarate.	
11	**Manutenzione**	**Adeguata**	**Nessuna**
		La manutenzione del sistema viene effettuata regolarmente da personale qualificato per garantirne l'efficienza e sicurezza dell'impianto.	
12	**Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)**	**Adeguata**	**Nessuna**
		Presente nomina a Project Automation SPA	
13	**Amministratore di sistema**	**Adeguata**	**Nessuna**
		Presente nomina a Project Automation SPA	
14	**Politica di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio di Polizia locale ha implementato un'organizzazione interna pienamente idonea a garantire l'adeguatezza della protezione dei dati personali sono state adeguatamente formalizzate le nomine e le istruzioni dei i soggetti interni autorizzati ad effettuare il trattamento dei dati personali.	
15	**Gestione delle politiche di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio di polizia pianifica periodicamente sessioni formative per il personale del Comando. Ultima sessione formativa effettuata nel 2° semestre 2023.	
16	**Gestire gli incidenti di sicurezza e le violazioni dei dati personali**	**Non Adeguata**	**Implementare**
		Non sono presenti procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.	Devono essere approvate e messe in atto una procedura e un'organizzazione operativa per rilevare le eventuali violazioni dei dati personali e gestire gli eventi che possono influire sulle libertà e sulla riservatezza degli interessati e per segnalare se del caso al Garante della protezione dei dati personali la violazione.
17	**Vigilanza sulla protezione dei dati**	**Non Adeguata**	**Implementare**
		Non risultano pianificati interventi di audit periodici atti a rilevare la corretta applicazione delle misure di sicurezza per la protezione dei dati personali.	Si consiglia di attuare audit periodici finalizzati a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.
18	**Lotta contro il malware**	**Adeguata**	**Nessuna**
		Antivirus di Windows attivo e aggiornamenti periodici attivi sui PC utilizzati per le visualizzazioni.	
19	**Gestione del personale**	**Adeguata**	**Nessuna**
		Tutte le attività che interessano la vds sono demandate al responsabile del Comando mediante decreto sindacale.	
20	**Prevenzione delle fonti di rischio**	**Adeguata**	**Nessuna**
		Seppur non presente in origine contestualmente alla valutazione d'impatto è stata condotta una puntuale valutazione dei rischi sul trattamento di videosorveglianza	

	Misura	Situazione in essere	Azione di miglioramento
21	**Gestione dei rischi**	**Non adeguata**	**Da implementare**
		Non è ancora stato definito un adeguato piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.	È consigliabile definire un piano di business continuity al fine di aumentare la capacità di continuare a disporre del servizio di videosorveglianza a livelli predefiniti accettabili a seguito di un incidente.
22	**Crittografia**	**Adeguata**	**Nessuna**
		Il sistema gestisce le immagini e le registra in formato proprietario con crittografia. Tutte le comunicazioni sono crittografate e i database sono protetti.	
23	**Controllo degli accessi logici**	**Adeguata**	**Nessuna**
		Sono utilizzate doppie credenziali di accesso alla piattaforma cloud ed il 2° accesso risulta essere a doppio fattore.	
24	**Gestione postazioni**	**Adeguata**	**Nessuna**
		Le postazioni o altri dispositivi, che consentono di accedere alle immagini, sono dotati di adeguati controlli logici di accesso per garantire che le persone che li utilizzano siano solo quelle autorizzate formalmente a effettuare i trattamenti di videosorveglianza.	
25	**Sicurezza dei canali informatici**	**Adeguata**	**Nessuna**
		Il collegamento tramite ADSL si realizza attraverso VPN protetta, firewall e credenziali personali di accesso alla piattaforma HIKCONNET	
26	**Controllo degli accessi fisici**	**Adeguata**	**Nessuna**
		Per le telecamere, antenne, router, switch, cabine stradali, ecc…., sono state adottate adeguate misure per limitare l'accesso a tale risorse alle sole persone formalmente autorizzate.	
27	**Sicurezza dell'hardware**	**Adeguata**	**Nessuna**
		Installazione in armadi protetti accessibili al solo personale autorizzato.	
28	**Protezione contro fonti di rischio non umane**	**Adeguata**	**Nessuna**
		Installazione eseguita con criterio per evitare danneggiamenti da parte degli eventi atmosferici.	
29	**Backup**	**Adeguato**	**Nessuna**
		Backup a cura del gestore cloud	

Valutazione sistema videosorveglianza e lettura targhe

Accesso illegittimo ai dati

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

Comunicazione dei dati non autorizzata, diffusione dei dati non autorizzata

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Malware, hacker, cancellazione involontaria, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Informativa di 1° livello, Informativa di 2° livello, Accesso alle immagini, Esercizio dei diritti degli interessati, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Amministratore di sistema, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Protezione contro fonti di rischio non umane,

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Accesso alle immagini, Esercizio dei diritti degli interessati, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Amministratore di sistema, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Protezione contro fonti di rischio non umane,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Limitato (Medio)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Importante (Probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Alto

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Accesso illegittimo ai dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Trascurabile (Improbabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Modifiche indesiderate dei dati

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

Attribuzione errata di un illecito, non attribuzione di un illecito commesso.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Hacker, malware, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna.

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Amministratore di sistema, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Amministratore di sistema, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei

canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Limitato (Medio)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Importante (Probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Alto

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Limitato (Poco probabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Perdita di dati

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

Attribuzione errata di un illecito, non attribuzione di un illecito commesso.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Hacker, malware, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna.

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Amministratore di sistema, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Amministratore di sistema, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Trascurabile (Lieve)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Massimo (Altamente probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Medio

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Limitato (Poco probabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Valutazione sistema fototrappole

Accesso illegittimo ai dati

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

Comunicazione dei dati non autorizzata, diffusione dei dati non autorizzata

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Malware, hacker, cancellazione involontaria, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Informativa di 1° livello, Informativa di 2° livello, Accesso alle immagini, Esercizio dei diritti degli interessati, Tracciabilità, Minimizzazione dei dati, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Accesso alle immagini, Esercizio dei diritti degli interessati, Tracciabilità, Minimizzazione dei dati, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Limitato (Medio)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Importante (Probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Alto

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Accesso illegittimo ai dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Trascurabile (Improbabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Modifiche indesiderate dei dati

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

Attribuzione errata di un illecito, non attribuzione di un illecito commesso.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Hacker, malware, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna.

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Tracciabilità, Minimizzazione dei dati, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Tracciabilità, Minimizzazione dei dati, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Limitato (Medio)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Importante (Probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Alto

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Medio)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Medio

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Limitato (Poco probabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Perdita di dati

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

Attribuzione errata di un illecito, non attribuzione di un illecito commesso.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Hacker, malware, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna.

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Tracciabilità, Minimizzazione dei dati, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Controllo

degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Tracciabilità, Minimizzazione dei dati, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Trascurabile (Lieve)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Massimo (Altamente probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Medio

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Importante (Probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Limitato (Poco probabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Valutazione sistema rilevamento rosso semaforico

Accesso illegittimo ai dati

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

Comunicazione dei dati non autorizzata, diffusione dei dati non autorizzata

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Malware, hacker, cancellazione involontaria, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Informativa di 1° livello, Informativa di 2° livello, Accesso alle immagini, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Protezione contro fonti di rischio non umane,

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Accesso alle immagini, Archiviazione, Minimizzazione dei dati, Manutenzione, Contratto con il responsabile del trattamento, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Limitato (Medio)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Importante (Probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Alto

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Accesso illegittimo ai dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Trascurabile (Improbabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Modifiche indesiderate dei dati

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

Attribuzione errata di un illecito, non attribuzione di un illecito commesso.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Hacker, malware, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna.

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane, Backup

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Archiviazione, Minimizzazione dei dati, Manutenzione, Contratto con il responsabile del trattamento, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei

canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Limitato (Medio)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Importante (Probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Alto

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Limitato (Poco probabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Perdita di dati

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

Attribuzione errata di un illecito, non attribuzione di un illecito commesso.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Hacker, malware, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna.

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Regolamento di Videosorveglianza, Registro dei trattamenti, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati(contratto con il responsabile del trattamento), Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane, Backup

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Regolamento di Videosorveglianza, Registro dei trattamenti, Archiviazione, Minimizzazione dei dati, Manutenzione, Contratto con il responsabile del trattamento, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Gestione del personale, Prevenzione delle fonti di rischio, Criptografia, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane, Backup

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Trascurabile (Lieve)

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

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Massimo (Altamente probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Medio

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Limitato (Poco probabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Data, 29 maggio 2025

Approvazione della valutazione di impatto da parte del Titolare del trattamento

Il Comandante di Polizia Locale - designato al trattamento dei dati personali afferente all'ufficio di Polizia Locale

Dott. Paolo Giana

PAOLO
GIANA
30.05.2025
13:37:52
GMT+02:00

(Firmato digitalmente)

In merito al parere sulla valutazione di impatto del tecnico che ha effettuato la valutazione

I tecnici che hanno redatto la valutazione

Liana Renacco

Enrico Capirone

(Firmato digitalmente)

Liana Caterina
Renacco
30.05.2025
17:11:46
GMT+01:00

Enrico
Capirone
31.05.2025
09:09:21
GMT+02:00

In merito al parere sulla valutazione di impatto del DPO/RDP

Il DPO
Dott. Paolo Tiberi

PAOLO
TIBERI

(Firmato digitalmente)