VIDEOSORVEGLIANZA

DATA PROTECTION IMPACT ASSESSEMENT

Comune di Montanaro

Città metropolitana di Torino

01 DICEMBRE 2021

REL. 1.0

Sommario

Documenti di riferimento

N. ALLEGATO	DERCRIZIONE	NOME FILE
01	Determina n. 341/2021 Incarico di valutazione di impatto sulla protezione dei dati DPIA per impianto di videosorveglianza del 1° ottobre 2021	ALLEGATO 01 DPIA - Determina affidamento incarico DPIA.pdf
02	Scheda tecnica Server - FUJITSU Desktop ESPRIMO P556/E85+	ALLEGATO 02 DPIA - Datasheet FUJITSU P556E85+.pdf
03	Genetec Security Center Installation Guide	ALLEGATO 03 DPIA - EN.Security Center Installation Guide 5.4 SR2.pdf
04	Scheda Genetec Security Center	ALLEGATO 04 DPIA - Scheda genetec-security-center.pdf
05	Scheda telecamera Datalab D113	ALLEGATO 05 DPIA -Datalab D113.pdf
06	Scheda telecamera DataLab D130-Z	ALLEGATO 06 DPIA -DataLab D130-Z.pdf
07	Scheda telecamera UNV_DPZ28_4MP_Motorized_VF	ALLEGATO 07 DPIA - UNV_DPZ28_4MP_Motorized_VF.pdf
08	Valutazione del livello di rischio per l'operazione di trattamento di videosorveglianza e misure di sicurezza tecniche e organizzative dell'ENISA (EUROPEAN UNION AGENCY FOR CYBERSECURITY)	ALLEGATO 08 DPIA - Enisa Risk assessment.pdf
09	Procedura operativa del trattamento di videosorveglianza	ALLEGATO 09 DPIA - PROCEDURA OPERATIVA DEL TRATTAMENTO DI VIDEOSORVEGLIANZA.docx
10	Facsimile registri	ALLEGATO 10 DPIA - FACSIMILE REGISTRI

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 e ne specifica i casi in cui è necessaria e ne procedimentalizza anche 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 scritto 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, perché il loro contenuto e il loro obiettivo è essenzialmente procedurale anche perché la DPIA è processo continuo è un esercizio fatto una volta per tutto, è in sostanza 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 conto 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 circa 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 è 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 che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli degli indagati. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in

[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.

cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

- **trattamenti di dati personali su larga scala**, il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:
  a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
  b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
  c) la durata, ovvero la persistenza, dell'attività di trattamento;
  d) la portata geografica dell'attività di trattamento[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 essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

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

[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 definisce la DPIA non è necessaria per i trattamenti che:

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

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

Alla luce della disamina di quanto disposto dal Regolamento (UE) 2016/679 all'articolo 35 e di quanto chiarito sia dal Garante della Protezione dei dati personali italiano e a livello UE dal Gruppo dell'articolo 29 è da 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 il 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 possa 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, i possibili impatti 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.

A tale valutazione complessiva effettuata utilizzando la metodologia CNIL in applicazione delle linee guida del WP29 è stato affiancato l'utilizzo dello strumento reso disponibile dall'ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY – specificamente realizzato per l'effettuazione della valutazione dei rischi.

Il risultato di tale valutazione è contenuto nell'ALLEGATO 08 DPIA - Enisa Risk assessment.pdf.

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

Il modello applicato da ENISA si basa su un approccio semplificato pensato per le PMI, adatto anche alle pubbliche amministrazioni locali, per aiutarle a valutare i relativi rischi per la sicurezza.

In quanto tale, l'approccio proposto non presenta una nuova metodologia di valutazione del rischio, ma si basa piuttosto sul lavoro esistente sul campo (CNIL – Managing Privacy Risks Methodology, ENISA - Raccomandazioni per una metodologia di valutazione della

[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.

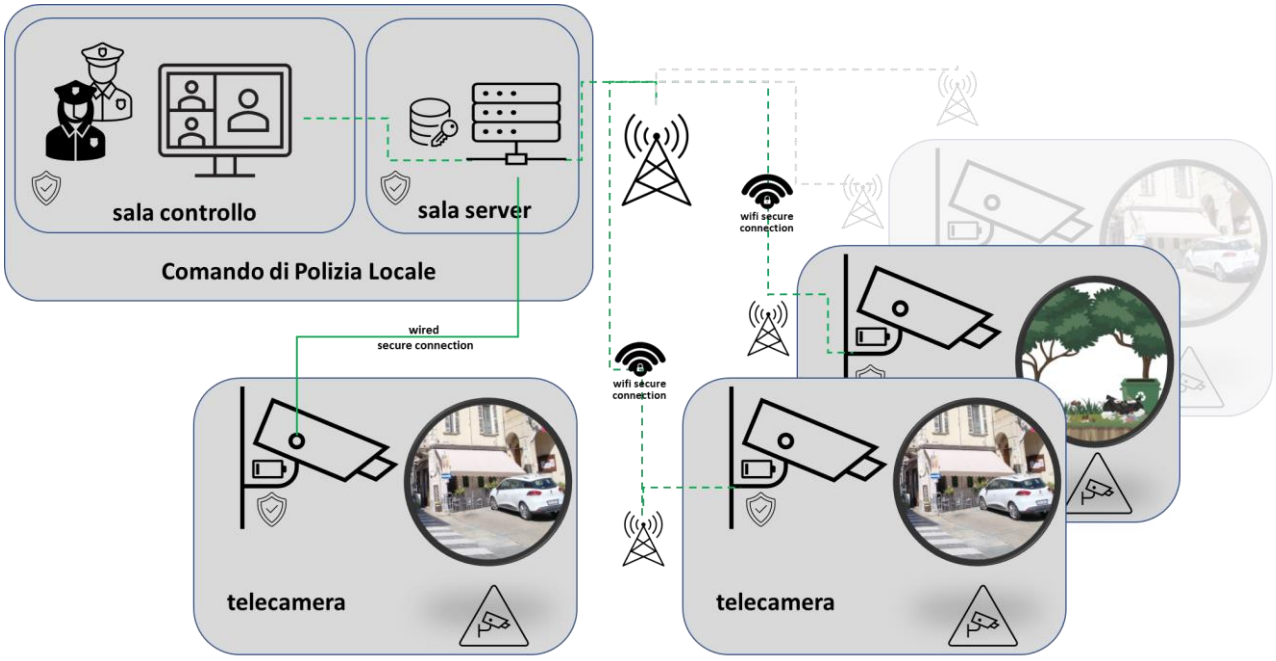
gravità delle violazioni dei dati personali, ENISA - Gestione dei rischi e valutazione dei rischi per le PMI) per fornire orientamenti alle PMI.

Questa specifico documento è incentrato esclusivamente sulla valutazione del rischio per la sicurezza nell'ambito delle operazioni di trattamento dei dati personali e non deve essere confuso con la valutazione dell'impatto sulla protezione dei dati (DPIA - Articolo 35 GDPR).

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

Validazione

Schema del sistema



Sala di controllo

La sala di controllo è collocata nell'ufficio della Polizia Locale che è una stanza chiusa ed è costituita da una postazione basata su un server con monitor.

La sala di controllo è chiusa a chiave e le chiavi sono in custodia del responsabile dell'ufficio di Polizia Locale.

La sala è protetta da inferiate alle finestre esterne e da doppia porta blindata all'ingresso.

Dotazione

Apparato	Quantità	Ubicazione:
Antenna Wireless FLY mod. nebula CPE 18	2	Piazza Donatori del sangue (1) Via Matteotti 13 (presso Palazzo Civico) (1)
Antenna Wireless UBIQUITY mod. Nanostation LOCO M5	2	Piazza L. MASSA (1) Via Matteotti 13 (presso Palazzo Civico) (1)
Antenna Wireless FLY mod. nebula CPE 23	2	Piazza Donatori del sangue (1) Via Mazzini 5 (presso Castello di Montanaro) (1)
Telecamera IP UNV_DPZ28_4MP_Motorized_VF	9	Piazza Donatori del sangue (4) Piazza L. MASSA (4)

		Via Matteotti 13 (presso ingresso del Palazzo Civico) (1)
Telecamera IP Datalab mod. D113	1	Via Matteotti 13 (presso cortile interno Palazzo Civico) (1)
Telecamera IP Datalab mod. D130 – Z	6	Via Mazzini 5 (presso Castello di Montanaro)
PC SERVER Fujitsu Siemens	1	Comando Polizia Municipale (sala operativa)
Software di gestione remota - GENETEC Security Agent 5.4	1	Comando Polizia Municipale (sala operativa)

Autorizzati al trattamento

1. Vitulli Alessio con qualifica di "Agente di Polizia Locale" e conseguentemente Agente di Polizia Giudiziari ai sensi dell'art. 57 CCP
2. Monica Capella – con qualifica dei "Agente di Polizia Locale" e conseguentemente Agente di Polizia Giudiziari ai sensi dell'art. 57 CCP

Responsabili Esterni

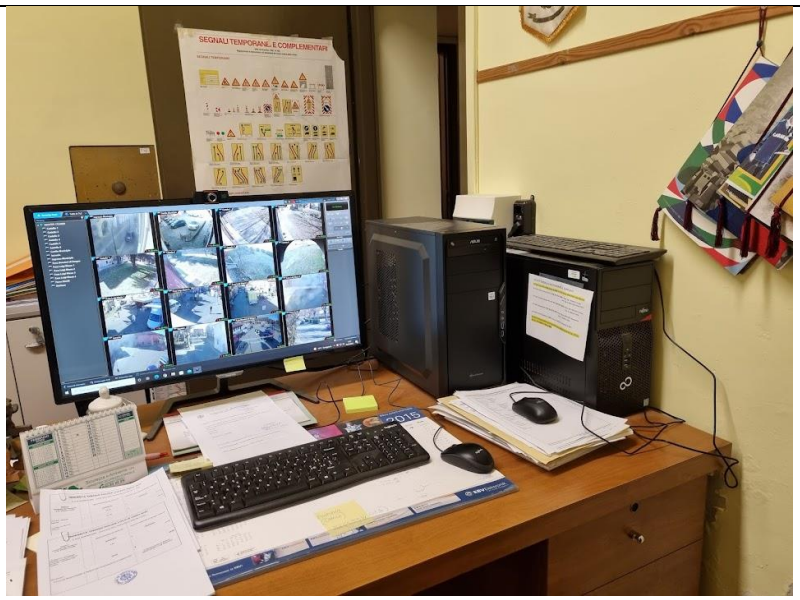
Ditta è **Hsl di Hyseni Adriano - C.so Peschiera, 325 - 10141 Torino – P.I. 09109740010**

Immagini dei disposti e della sala operativa

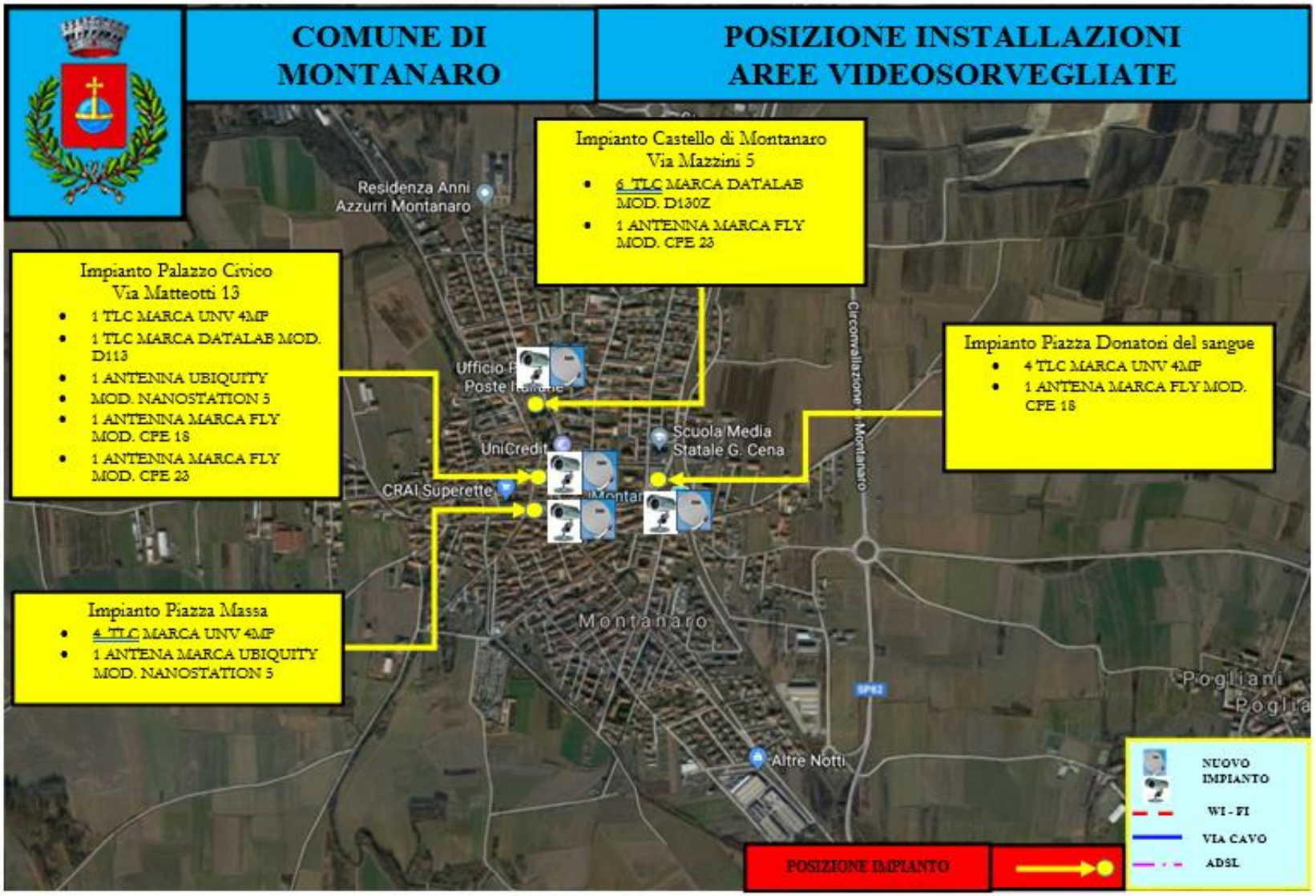
TELECAMERA DATALAB D113FD	
	– Telecamera ip Full HD bullet con risoluzione 1.3MP per uso interno ed esterno, H.264, day&night con led IR integrati per visione notturna fino a 30 metri, ottica fissa 3.6mm, WDR, 12V e PoE. – Telecamera bullet da interno/esterno – Risoluzione 1.3 megapixel a 25 frame al secondo – Sensore CMOS 1/3" a scansione progressiva – Tecnologia video MJPEG, H264 con supporto flussi video asincroni (dual-stream) – Sensibilità 0.005 Lux F1.2, 0 Lux con led IR attivi – Filtro day&night meccanico per visione notturna (IR Cut Filter) – Distanza led IR fino a 25 metri – Obiettivo 3.6mm, F1.2 – Angolo di visualizzazione orizzontale pari 74° – Funzioni BLC, 3D DNR, Motion Detection, WDR – Compatibile con protocollo Onvif – Doppia alimentazione 12v DC e PoE 802.3af Class 3 (8w) – Temperatura operativa da -40°C a +60°C (RH da 0% a 95% non-condensing) – Certificazione CE, FCC, IP66
TELECAMERA DATALAB 130-Z	
	– Telecamera ip da esterno, 3MP, H.264, day&night con led IR integrati per visione notturna fino a 35 metri, ottica varifocale autofocus 2.8-12mm, WDR, 12V e PoE. – Telecamera ip Full HD bullet con ottica motorizzata e risoluzione 3 megapixel per uso esterno, resistente alle intemperie (IP66). – Sensore CMOS da 1/2.5" a scansione progressiva. – Filtro day&night meccanico per visione notturna, fino a 0 LUX mediante illuminatore led IR adattivi (portata 35m) integrati. – Funzionalità AWB e AGC manuale o auto, 3D DNR, Flickerless e WDR. Compressione H.264 e MJPEG selezionabili con possibilità di invio di flussi video multipli (dual stream). – Fino a 20 fps alla risoluzione di 2048x1536 pixel, fino a 30 fps alla risoluzione Full HD di 1920x1080 pixel, HD di 1280x720 pixel e VGA di 640x480 pixel. – Lente varifocale 2.8~12 mm, F1.4 motorizzata con controllo remoto via software per messa a fuoco, zoom, iris. – Angolo di visualizzazione orizzontale da 86° a 26°, doppia alimentazione 12 V DC e PoE (802.3af max. 15,4W Class3). – Alloggiamento in alluminio e tettuccio parasole. – Staffa con passaggio interno e protetto dei cavi di collegamento ed alimentazione inclusa. – Licenza software Data Lab VMS versione POP inclusa.
TELECAMERA Telecamera IP UNV_ IPC2324EBR5-DPZ28 _4MP_Motorized_VF	
	– Optics: Day/night functionality; Smart IR, up to 50m (164 ft) IR distance; Up to 120 dB Optical WDR(Wide Dynamic Range); 2D/3D DNR (Digital Noise Reduction) – Compression: Ultra 265,H.265, H.264, MJPEG; Embedded smart algorithm; Triple streams; ROI (Region of Interest); 9:16 corridor mode; Customized OSD; – Network: ONVIF Conformance; – Structure: Wide temperature range -35°C to 60°C (-31°F to 140°F); Wide voltage range of ±25%; IP67; 3-Axis

SERVER - FUJITSU ESPRIMO P556/E85+

SALA OPERATIVA PRESSO L'UFFICIO DELLA POLIZIA LOCALE



Schema generale siti di installazione



Siti di installazione delle telecamere e caratteristiche impianto

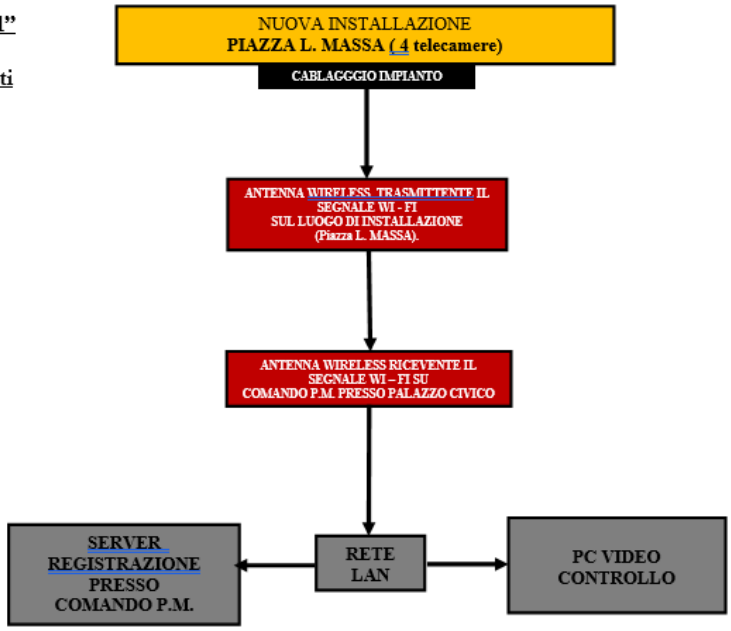
Piazza Luigi Massa

ALLEGATO " B" – INSTALLAZIONE 4 TELECAMERE IN PIAZZA L. MASSA

IMPIANTO DI VIDEOSORVEGLIANZA
COMUNE DI MONTANARO – Impianto PIAZZA L. MASSSA.

ALLEGATO " A1"

Percorso invio dati



Antenne riceventi

SCHEDA TECNICA DELL'IMPIANTO

(in caso di impianto con più frequenze da compilarsi una per ogni frequenza)

DATI ANAGRAFICI							
PROPRIETARIO	COMUNE DI MONTANARO - Provincia di Torino						
Via	Matteotti					N.	13
CITTA	MONTANARO	PROV.	TO	CAP	10017	TEL.	011 9160102
EMITTENTE (MANUTENTORE)	H.S.L. Impianti - C.so Peschiera, 325 - Torino						
LOCALITA' IMPIANTO	MONTANARO (TO)						
Via	Matteotti					N.	13
FOGLIO		MAPPALE					
(Da compilare nel caso in cui l'impianto sia situato in luogo non definito da via e numero civico)							
COMUNE	MONTANARO					PROV.	TO
QUOTA slm INSTALLAZIONE	211						mt
COORDINATE DELL'IMPIANTO (UTM ED 1950 o Gauss Boaga): 5009456 0409952 32T							
X	0409952			; Y	5009456		

DATI TECNICI						
(In caso di impianti di telefonia da compilarsi per ogni scheda)						
☒	**NUOVO IMPIANTO**					
☐	MODIFICA IMPIANTO: IMPLEMENTAZIONE					
☐	SOSTITUZIONE (barrare)					
FREQUENZA	5.470	MHz				
MULTIPLEXING	☒ NO					
	SI CON				(barrare e specificare)	
ALTEZZA CENTRO ELETTRICO DEL SISTEMA IRRADIANTE:						
da terra	5	mt	dal basamento (se posto su edificio)		----	mt
POTENZA AL CONNETTORE D'ANTENNA			0,1		Watt	
DIREZIONE			184		gradi nord	
MARCA ANTENNA			UBIQUITY			
MODELLO ANTENNA			NANO STATION LOCO M5			
GUADAGNO SISTEMA IRRADIANTE			13		dBi	
TIL T MECCANICO			-3		gradi	
TIL T ELETTRICO			18		gradi	
TIL T COMPLESSIVO			15		gradi	
POLARIZZAZIONE			LINEARE			
NUMERO MAX DI PORTANTI			2			

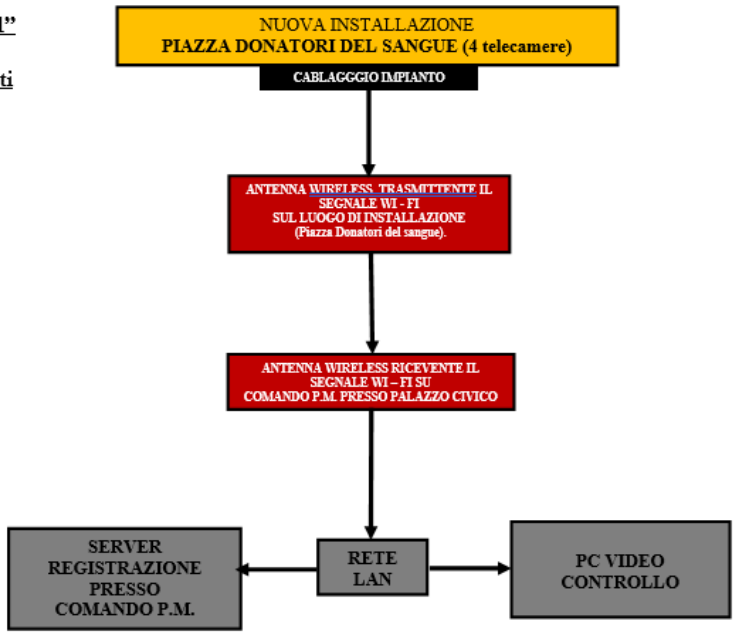

COMUNE DI MONTANARO
IMPIANTO WI – FI
PIAZZA L. MASSA
Impianto Palazzo Civico
Via Matteotti 13
(sala operativa Comando P.M.)
• 1 ANTENNA MARCA UBIQUITY MOD. NANOSTATION LOCO M5 (ricevente impianto WI-FI)
SERVER SALA OPERATIVA
Impianto Piazza Massa
• 4 TLC MARCA UNV 4MP
• 1 ANTENNA MARCA UBIQUITY MOD. NANOSTATION LOCO M5 (trasmittente impianto WI-FI)
NUOVO IMPIANTO
WI - FI
VIA FILO
ADSL
Via Silvio Pellico
Via Papa Giovanni XXIII
Ufficio Postale Poste Italiane
Via Alcide De Gasperi
Via dei Calzolai
Parco del Castello
Via Carlo Ubertini
Torre della Zecca
Scuola Media Statale G. Cena
L' Innominata
Alimentari Regis
Banca Sella
CRAI Superette
Citta' Futura S.R.L.
Supermercato
Montanaro
Via Roma
Via Tremoli
Bollero Mauro
Via Goito
Via Piave

Piazza Donatori del Sangue

IMPIANTO DI VIDEOSORVEGLIANZA
COMUNE DI MONTANARO – Impianto PIAZZA DONATORI DEL SANGUE.

ALLEGATO " A1"

Percorso invio dati



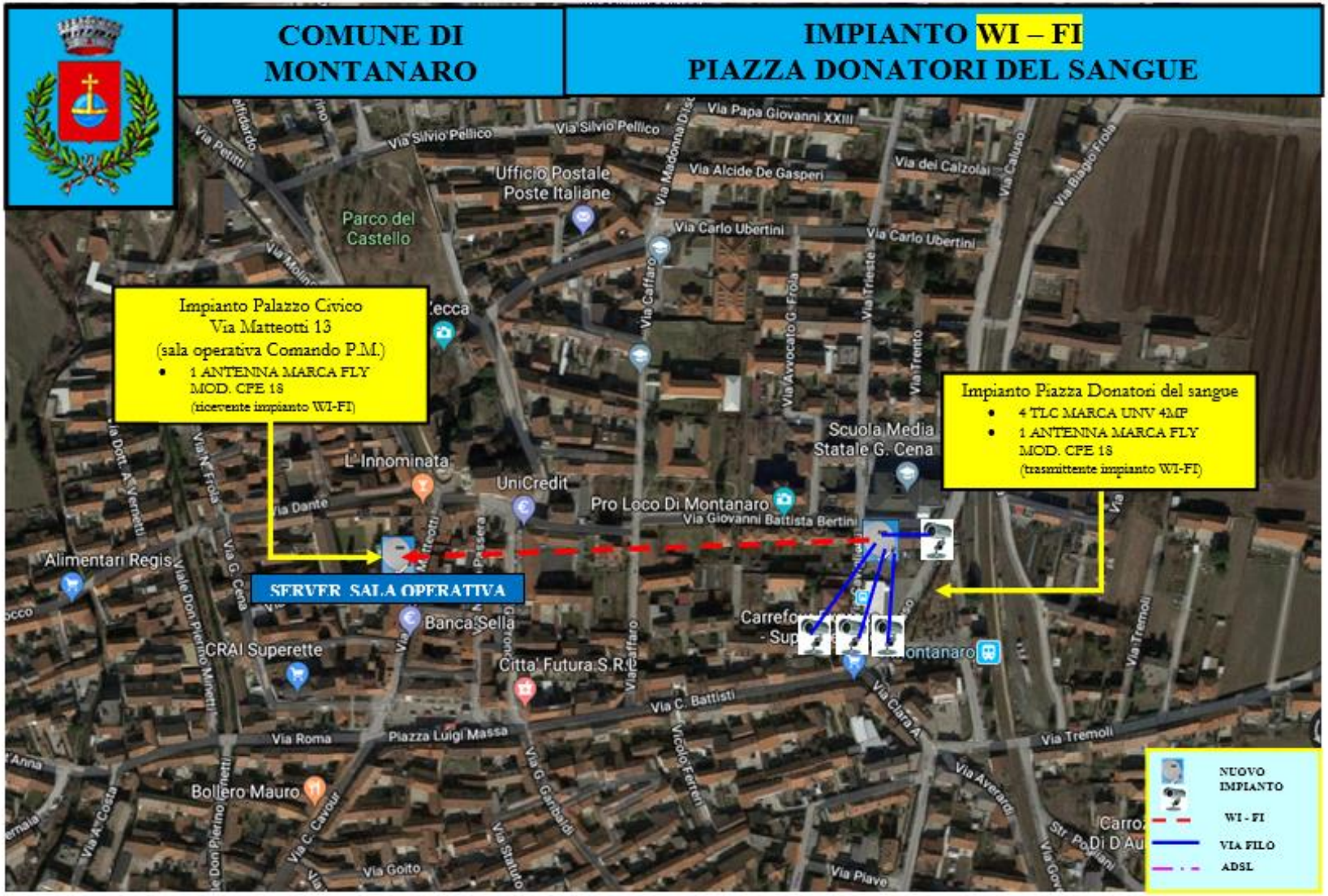
Antenne riceventi

SCHEDA TECNICA DELL'IMPIANTO

(in caso di impianto con più frequenze da compilarsi una per ogni frequenza)

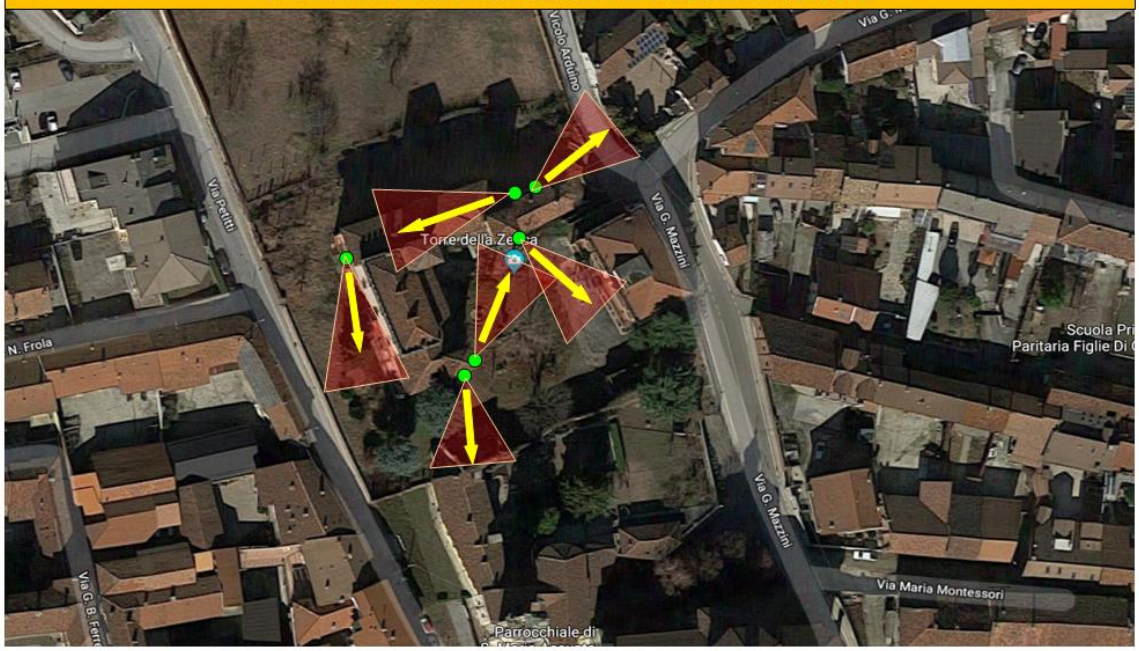
DATI ANAGRAFICI							
PROPRIETARIO	COMUNE DI MONTANARO - Provincia di Torino						
Via	Matteotti					N.	13
CITTA	MONTANARO	PROV.	TO	CAP	10017	TEL.	011 9160102
EMITTENTE (MANUTENTORE)	H.S.L. Impianti - C.so Peschiera, 325 - Torino						
LOCALITA' IMPIANTO	MONTANARO (TO)						
Via	Matteotti					N.	13
FOGLIO		MAPPALE					
(Da compilare nel caso in cui l'impianto sia situato in luogo non definito da via e numero civico)							
COMUNE	MONTANARO					PROV.	TO
QUOTA slm INSTALLAZIONE	211						mt
COORDINATE DELL'IMPIANTO (UTM ED 1950 o Gauss Boaga): 5009456 0409952 32T							
X	0409952	; Y	5009456				

DATI TECNICI (In caso di impianti di telefonia da compilarsi per ogni scheda)					
☒	**NUOVO IMPIANTO**				
☐	MODIFICA IMPIANTO: IMPLEMENTAZIONE				
☐	SOSTITUZIONE (barrare)				
FREQUENZA	5.600	MHz			
MULTIPLEXING	☒ NO				
	SI CON			(barrare e specificare)	
ALTEZZA CENTRO ELETTRICO DEL SISTEMA IRRADIANTE:					
da terra	18	mt	dal basamento (se posto su edificio)	2	mt
POTENZA AL CONNETTORE D'ANTENNA	0,1	Watt			
DIREZIONE	100	gradi nord			
MARCA ANTENNA	FLY				
MODELLO ANTENNA	NEBULA CPE 18				
GUADAGNO SISTEMA IRRADIANTE	18	dBi			
TIL T MECCANICO	-3	gradi			
TIL T ELETTRICO	18	gradi			
TIL T COMPLESSIVO	15	gradi			
POLARIZZAZIONE	LINEARE				
NUMERO MAX DI PORTANTI	2				


COMUNE DI MONTANARO
IMPIANTO WI – FI
PIAZZA DONATORI DEL SANGUE
Impianto Palazzo Civico
Via Matteotti 13
(sala operativa Comando P.M.)
• 1 ANTENNA MARCA FLY MOD. CPE 18
(ricevente impianto WI-FI)
Impianto Piazza Donatori del sangue
• 4 TLC MARCA UNV 4MP
• 1 ANTENNA MARCA FLY MOD. CPE 18
(trasmittente impianto WI-FI)
SERVER SALA OPERATIVA
NUOVO IMPIANTO
WI - FI
VIA FILO
ADSL
Via Silvio Pellico
Via Papa Giovanni XXIII
Via Alcide De Gasperi
Via dei Calzolai
Via Carlo Ubertini
Ufficio Postale Poste Italiane
Parco del Castello
Scuola Media Statale G. Cena
L'Innominata
UniCredit
Pro Loco Di Montanaro
Via Giovanni Battista Bertini
Alimentari Regis
Banca Sella
CRAI Superette
Citta' Futura S.R.L.
Via Roma
Piazza Luigi Massa
Via C. Battisti
Via Tremoli
Bollero Mauro
Via Goito
Via Piave

Castello di Montanaro

ALLEGATO " B" – INSTALLAZIONE PRESSO CASTELLO DI MONTANARO
N° 6 TELECAMERE CON VISUALE INTERNA ALL'EDIFCIO

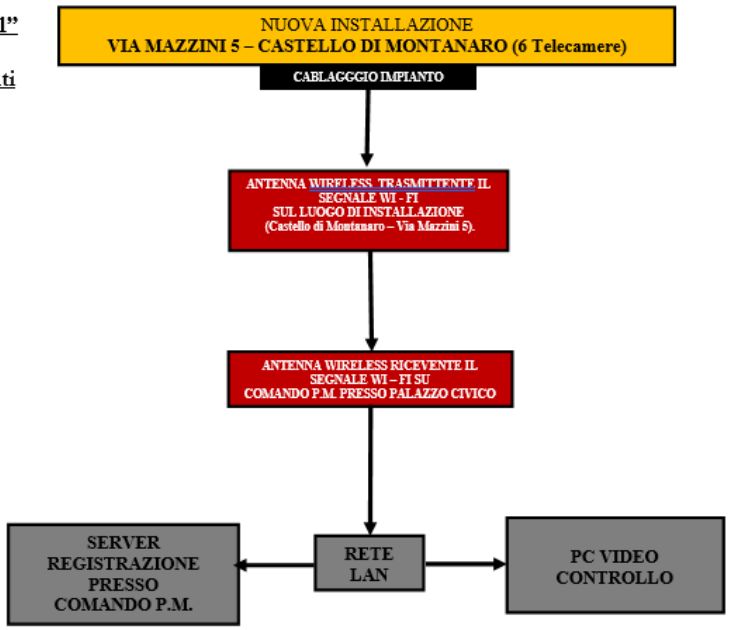


LEGENDA: POSIZIONE TELECAMERA — AREA RICOPERTA — DIREZIONE DELLA VISUALE

IMPIANTO DI VIDEOSORVEGLIANZA
COMUNE DI MONTANARO – Impianto CASTELLO DI MONTANARO – Via Mazzini 5.

ALLEGATO " A1"

Percorso invio dati



Antenne riceventi

SCHEDA TECNICA DELL'IMPIANTO

(in caso di impianto con più frequenze da compilarsi una per ogni frequenza)

DATI ANAGRAFICI							
PROPRIETARIO	COMUNE DI MONTANARO - Provincia di Torino						
Via	Matteotti					N.	13
CITTA	MONTANARO	PROV.	TO	CAP	10017	TEL.	011 9160102
EMITTENTE (MANUTENTORE)	H.S.L. Impianti - C.so Peschiera, 325 - Torino						
LOCALITA' IMPIANTO	MONTANARO (TO)						
Via	Matteotti					N.	13
FOGLIO		MAPPALE					
(Da compilare nel caso in cui l'impianto sia situato in luogo non definito da via e numero civico)							
COMUNE	MONTANARO					PROV.	TO
QUOTA slm INSTALLAZIONE	211						mt
COORDINATE DELL'IMPIANTO (UTM ED 1950 o Gauss Boaga): 5009456 0409952 32T							
X	0409952	; Y	5009456				

DATI TECNICI					
(In caso di impianti di telefonia da compilarsi per ogni scheda)					
☒	**NUOVO IMPIANTO**				
☐	MODIFICA IMPIANTO: IMPLEMENTAZIONE				
☐	SOSTITUZIONE (barrare)				
FREQUENZA	5.600	MHz			
MULTIPLEXING	☒ NO				
	SI CON			(barrare e specificare)	
ALTEZZA CENTRO ELETTRICO DEL SISTEMA IRRADIANTE:					
da terra	18	mt	dal basamento (se posto su edificio)	2	mt
POTENZA AL CONNETTORE D'ANTENNA		0,1	Watt		
DIREZIONE		50	gradi nord		
MARCA ANTENNA		FLY			
MODELLO ANTENNA		NEBULA CPE 23			
GUADAGNO SISTEMA IRRADIANTE		23	dBi		
TIL T MECCANICO		22°	gradi		
TIL T ELETTRICO		15°	gradi		
TIL T COMPLESSIVO		37°	gradi		
POLARIZZAZIONE		LINEARE			
NUMERO MAX DI PORTANTI		2			


COMUNE DI MONTANARO
IMPIANTO WI – FI
CASTELLO DI MONTANARO – Via Mazzini 5
Impianto Castello di Montanaro
In Via Mazzini 5
6 TLC MARCA DATALAB MOD. D130-Z
1 ANTENNA MARCA FLY MOD. CPE 23
(trasmittente segnale WI- FI)
SERVER SALA OPERATIVA
Impianto Palazzo Civico
Via Matteotti 13 (sala operativa Comando P.M.)
1 ANTENNA MARCA FLY MOD. CPE 23
(ricevente segnale WI-FI)
Parco del Castello
Scuola Media Statale G. Cena
Pro Loco Di Montanaro
UniCredit
Banca Sella
Carrefour Express Supermercato
Montanaro
Alimentari Regis
Bollero Mauro
Piazza Luigi Massa
Via Dante
Via Giovanni Battista Bertini
Via Silvio Pellico
Via Carlo Ubertini
Via dei Calzolai
Via Tremoli
Via Goito
Via Piave
NUOVO IMPIANTO
WI - FI
VIA FILO
ADSL

Palazzo Civico

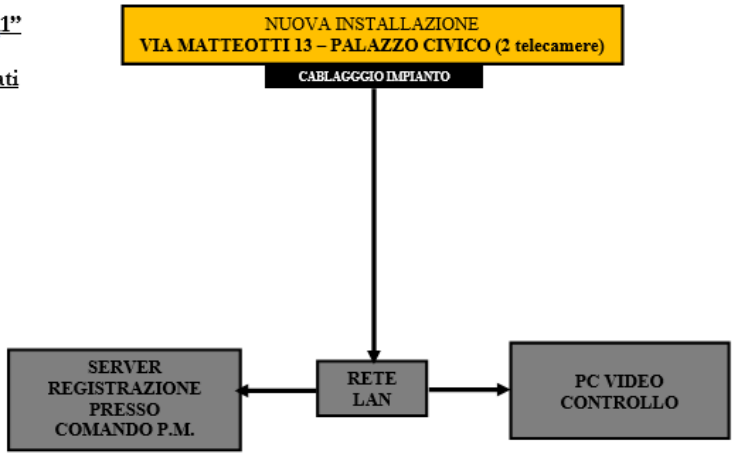
ALLEGATO " B" – INSTALLAZIONE PRESSO PALAZZO CIVICO - N° 2 TELECAMERE (INGRESSO PALAZZO CIVICO E CORTILE INTERNO)

LEGENDA: POSIZIONE TELECAMERA — AREA RICOPERTA — DIREZIONE DELLA VISUALE

IMPIANTO DI VIDEOSORVEGLIANZA
COMUNE DI MONTANARO – Impianto PALAZZO CIVICO – Via Matteotti 13.

ALLEGATO " A1"

Percorso invio dati



Antenne trasmittenti

DATI ANAGRAFICI								
PROPRIETARIO	COMUNE DI MONTANARO - Provincia di Torino							
Via	Matteotti					N.	13	
CITTA	MONTANARO	PROV.	TO	CAP	10017	TEL.	011 9160102	
EMITTENTE (MANUTENTORE)	H.S.L. Impianti - C.so Peschiera, 325 - Torino							
LOCALITA' IMPIANTO	MONTANARO (TO)							
Piazza	L. Massa angolo Via Matteotti					N.	----	
FOGLIO		MAPPALE						
(Da compilare nel caso in cui l'impianto sia situato in luogo non definito da via e numero civico)								
COMUNE	MONTANARO					PROV.	TO	
QUOTA slm INSTALLAZIONE	212						mt	
COORDINATE DELL'IMPIANTO (UTM ED 1950 o Gauss Boaga): 5009404 0409953 32T								
X	0409953	; Y	5009404					

DATI TECNICI					
(In caso di impianti di telefonia da compilarsi per ogni scheda)					
☒	**NUOVO IMPIANTO**				
☐	MODIFICA IMPIANTO: IMPLEMENTAZIONE				
☐	SOSTITUZIONE (barrare)				
FREQUENZA	5.470	MHz			
MULTIPLEXING	☒ NO				
	SI CON			(barrare e specificare)	
ALTEZZA CENTRO ELETTRICO DEL SISTEMA IRRADIANTE:					
da terra	5	mt	dal basamento (se posto su edificio)	----	mt
POTENZA AL CONNETTORE D'ANTENNA		0,1	Watt		
DIREZIONE		4	gradi nord		
MARCA ANTENNA		UBIQUITY			
MODELLO ANTENNA		NANO STATION LOCO M5			
GUADAGNO SISTEMA IRRADIANTE		13	dBi		
TIL T MECCANICO		-3	gradi		
TIL T ELETTRICO		18	gradi		
TIL T COMPLESSIVO		15	gradi		
POLARIZZAZIONE		LINEARE			
NUMERO MAX DI PORTANTI		2			

SCHEDA TECNICA DELL'IMPIANTO

(in caso di impianto con più frequenze da compilarsi una per ogni frequenza)

DATI ANAGRAFICI							
PROPRIETARIO	COMUNE DI MONTANARO - Provincia di Torino						
Via	Matteotti					N.	13
CITTA	MONTANARO	PROV.	TO	CAP	10017	TEL.	011 9160102
EMITTENTE (MANUTENTORE)	H.S.L. Impianti - C.so Peschiera, 325 - Torino						
LOCALITA' IMPIANTO	MONTANARO (TO)						
Piazza	Donatori del sangue					N.	----
FOGLIO		MAPPALE					
(Da compilare nel caso in cui l'impianto sia situato in luogo non definito da via e numero civico)							
COMUNE	MONTANARO					PROV.	TO
QUOTA slm INSTALLAZIONE	210						mt
COORDINATE DELL'IMPIANTO (UTM ED 1950 o Gauss Boaga): 5009441 0410322 32T							
X	0410322	; Y	5009441				

DATI TECNICI				
(In caso di impianti di telefonia da compilarsi per ogni scheda)				
☒	**NUOVO IMPIANTO**			
☐	MODIFICA IMPIANTO: IMPLEMENTAZIONE			
☐	SOSTITUZIONE (barrare)			
FREQUENZA	5.600	MHz		
MULTIPLEXING	☒ NO			
	SI CON		(barrare e specificare)	
ALTEZZA CENTRO ELETTRICO DEL SISTEMA IRRADIANTE:				
da terra	5 mt	dal basamento (se posto su edificio)	/	mt
POTENZA AL CONNETTORE D'ANTENNA		0,1	Watt	
DIREZIONE		280 °	gradi nord	
MARCA ANTENNA		FLY		
MODELLO ANTENNA		NEBULA CPE 18		
GUADAGNO SISTEMA IRRADIANTE		18	dBi	
TIL T MECCANICO		-3	gradi	
TIL T ELETTRICO		18	gradi	
TIL T COMPLESSIVO		15	gradi	
POLARIZZAZIONE		LINEARE		
NUMERO MAX DI PORTANTI		2		

SCHEDA TECNICA DELL'IMPIANTO

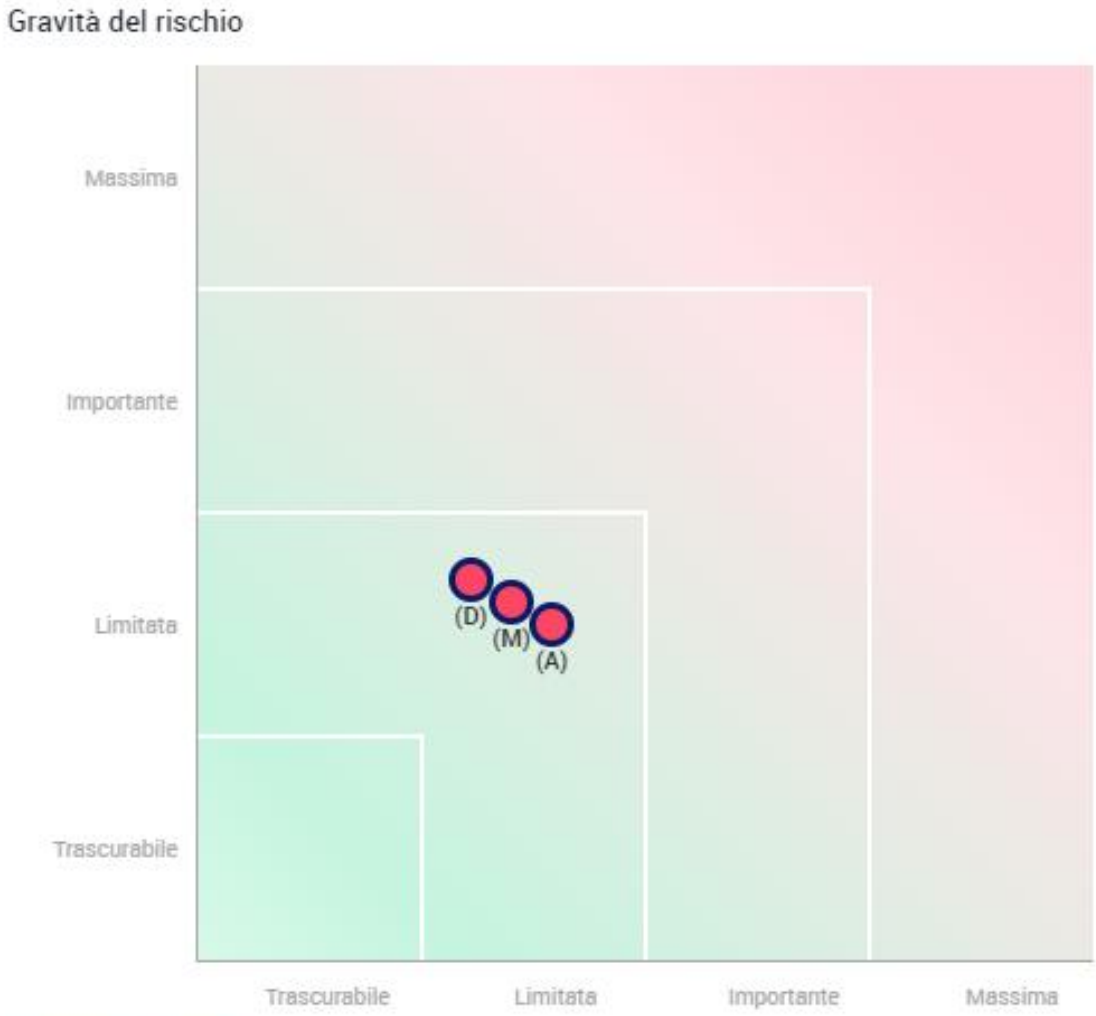
(in caso di impianto con più frequenze da compilarsi una per ogni frequenza)

DATI ANAGRAFICI							
PROPRIETARIO	COMUNE DI MONTANARO - Provincia di Torino						
Via	Matteotti					N.	13
CITTA	MONTANARO	PROV.	TO	CAP	10017	TEL.	011 9160102
EMITTENTE (MANUTENTORE)	H.S.L. Impianti - C.so Peschiera, 325 - Torino						
LOCALITA' IMPIANTO	MONTANARO (TO)						
Via	Mazzini					N.	5
FOGLIO		MAPPALE					
(Da compilare nel caso in cui l'impianto sia situato in luogo non definito da via e numero civico)							
COMUNE	MONTANARO					PROV.	TO
QUOTA slm INSTALLAZIONE	213						mt
COORDINATE DELL'IMPIANTO (UTM ED 1950 o Gauss Boaga): 5009633 0409973 32T							
X	0409973	; Y	50009633				

DATI TECNICI					
(In caso di impianti di telefonia da compilarsi per ogni scheda)					
☒	**NUOVO IMPIANTO**				
☐	MODIFICA IMPIANTO: IMPLEMENTAZIONE				
☐	SOSTITUZIONE (barrare)				
FREQUENZA	5.600	MHz			
MULTIPLEXING	☒ NO				
	SI CON			(barrare e specificare)	
ALTEZZA CENTRO ELETTRICO DEL SISTEMA IRRADIANTE:					
da terra	20	mt	dal basamento (se posto su edificio)	2	mt
POTENZA AL CONNETTORE D'ANTENNA		0,1	Watt		
DIREZIONE		230	gradi nord		
MARCA ANTENNA		FLY			
MODELLO ANTENNA		NEBULA CPE 23			
GUADAGNO SISTEMA IRRADIANTE		23	dBi		
TIL T MECCANICO		22°	gradi		
TIL T ELETTRICO		15°	gradi		
TIL T COMPLESSIVO		37°	gradi		
POLARIZZAZIONE		LINEARE			
NUMERO MAX DI PORTANTI		2			


COMUNE DI MONTANARO
IMPIANTO (CABLATO)
PALAZZO CIVICO – Via Matteotti 13
Impianto Palazzo Civico
Via Matteotti 13
(sala operativa Comando P.M.)
• 1 TLC MARCA UNV MOD. 4MP
• 1 TLC MARCA DATALAB MOD. D113
SERVER SALA OPERATIVA
Parco del Castello
Ufficio Postale Poste Italiane
L' Innominata
UniCredit
Pro Loco Di Montanaro
Scuola Media Statale G. Cena
Alimentari Regis
Banca Sella
CRAI Superette
Citta' Futura S.R.L.
Bollero Mauro
Via Silvio Pellico
Via Papa Giovanni XXIII
Via Alcide De Gasperi
Via dei Calzolai
Via Carlo Ubertini
Via Caffaro
Via Trieste
Via Trento
Via Caluso
Via Ivrea
Via Tremoli
Via Roma
Piazza Luigi Massa
Via C. Battisti
Via Giovanni Battista Bertini
Via Avvocato Taraglio
Via Dante
Via Goito
Via Piave
Montanaro
NUOVO IMPIANTO
WI - FI
VIA FILO
ADSL

Mappatura dei rischi



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Panoramica

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 individuati e che le misure tecniche adottate sono rivolte al fine di minimizzarne la probabilità che si verifichino e l'impatto che potrebbero avere sugli interessati.

Panoramica

Principi fondamentali

Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Informativa
Raccolta del consenso
Diritto di accesso e diritto alla portabilità dei dati
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione
Responsabili del trattamento
Trasferimenti di dati

Misure esistenti o pianificate

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

Rischi

Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure migliorabili

Misure accettabili

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 pianificare

Le misure tecniche che sono state implementate si ritengono coerenti e adeguate al trattamento in oggetto, tuttavia, sono state individuate alcune misure tecniche che se fossero implementate eleverebbero ulteriormente la sicurezza del trattamento e le garanzie per i diritti e le libertà degli interessati.

Rispetto alle misure organizzative si precisa che forma parte integrante delle misure di sicurezza ai fini della presente la procedura operativa a cui devono attenersi gli addetti interni autorizzati nell'effettuazione dei trattamenti.

Crittografia

Piano d'azione / misure correttive:

Implementare la criptografia delle immagini contenute sull'HD.

Commento di valutazione:

- è da considerare che il server è collocato all'interno dell'ufficio di Polizia Locale, chiuso a chiave e dotato di inferiate alle finestre;
- inoltre, la rete delle videosorveglianza è una rete dedicata separata da quella del Comune e l'accesso al server dall'esterno per la manutenzione da parte della ditta debitamente nominata responsabile del trattamento avviene attraverso sw di accesso remoto che viene attivato dal personale interno solo per il periodo necessario; il rischio di accesso alle immagini (data breach) è quindi limitato, ciononostante permane un rischio relativo alla possibilità derivante da fonte umana che riuscendo ad accedere al locale potrebbe trafugare il server e successivamente accedere ai filmati;
- attraverso l'implementazione della criptografia questo rischio residuo verrebbe ulteriormente ridotto.

Backup

Piano d'azione / misure correttive:

Dotare il sistema di un sistema per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.

Commento di valutazione:

Il Backup dei dati ridurrebbe il rischio di perdita dei dati di registrazione in caso di danneggiamento dell'HD del server.

Si consideri che nello specifico la perdita dei danni andrebbe principalmente a danno del Comune e della collettività più che a danno dell'interessato inteso come soggetto che commette un eventuale illecito le cui immagini andrebbero perse in caso di danneggiamento dell'HD del server.

Rischi

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

Parere del DPO e degli interessati

Nome del DPO/RPD

Enrico Capirone

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Seppure il tipo di trattamento in se, gestione di sequenze di immagini acquisite in zone aperte al pubblico attraverso telecamere segnalate con cartelli, trasmissione delle immagini tramite rete wireless dedicata e sicura e relativa memorizzazione delle immagini su un server dedicato 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, possa rappresentare un rischio relativo ai diritti e libertà dei soggetti interessati qualificabile come elevato, si ritiene che i dispositivi e le misure tecniche ed organizzative individuate e adottate fin dalla progettazione e che saranno utilizzate durante l'esercizio siano adeguate a mitigare il rischio portando il rischio residuale ad un livello che può essere qualificato come residuale basso.

Come indicato nelle misure organizzative relative alla gestione del personale deve essere adottata una procedura operativa dettagliata che sia vincolante per gli addetti preposti al trattamento (si veda "ALLEGATO 09 DPIA – PROCEDURA OPERATIVA DEL TRATTAMENTO DI VIDEOSORVEGLIANZA").

Tuttavia, per ridurre ulteriormente il rischio si consiglia di valutare l'implementazione della ulteriore misura di sicurezza indicata nel piano d'azione.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si ritiene utile per questo trattamento richiedere il parere degli interessati in quanto è un trattamento finalizzato a limitare e reprimere comportamenti illeciti. Inoltre, è un trattamento finalizzato alla sicurezza urbana attuato con modalità analoga a quanto già effettuato in numerosissimi contesti analoghi.

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. attivare misure di prevenzione e sicurezza sul territorio Comunale;
b. la protezione e 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. prevenire eventuali atti di vandalismo o danneggiamento agli immobili ed in particolare al patrimonio comunale e di disturbo alla quiete pubblica;
d. la protezione della proprietà;
e. le attività di rilevazione, prevenzione e controllo delle infrazioni, nel quadro delle competenze attribuite dalla legge;
f. l'acquisizione di fonti di prove in ambito delle attività di polizia amministrativa;
g. per 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;
h. monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
i. verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;

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 (UY) 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"	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.

DM del Ministro dell'Interno del 09/08/2008	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)	Incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione.
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", convertito con modificazioni dalla L. 18 aprile 2017, n. 48 (in G.U. 21/04/2017, n. 93).	Disposizioni in materia di sicurezza delle città
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
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

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 trattati 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. attivare misure di prevenzione e sicurezza sul territorio Comunale;
b. la protezione e 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. prevenire eventuali atti di vandalismo o danneggiamento agli immobili ed in particolare al patrimonio comunale e di disturbo alla quiete pubblica;
d. la protezione della proprietà;
e. le attività di rilevazione, prevenzione e controllo delle infrazioni, nel quadro delle competenze attribuite dalla legge;
f. l'acquisizione di fonti di prove in ambito delle attività di polizia amministrativa;
g. per 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;
h. monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
i. verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;

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 cui viene effettuato il trattamento dei dati presenta le seguenti caratteristiche salienti:

1. l'impianto di videosorveglianza è costituito da telecamere fisse che sono state posizionate dopo attento studio e progettazione;
2. l'impianto acquisisce e memorizza in modo continuato su apposito server le immagini relative alle diverse zone sottoposte a monitoraggio;
3. le telecamere sono posizione su pali difficilmente accessibili e in ogni caso non memorizzano immagini su memoria locale ma le trasmettono tramite una rete wireless sicura al server custodito all'interno dell'ufficio di Polizia Locale.
4. In prossimità delle zone sottoposte a monitoraggio sono apposti cartelli di segnalazione a norma delle vigenti disposizioni normative.

Il trattamento dei dati personali viene 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 non sono registrate nella memoria della telecamera ma immediatamente trasmesse attraverso rete wireless dedicata e sicura (wpa2-psk) al server collocato e custodito all'interno dell'ufficio di Polizia Locale.
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 in cui, il registro, dovesse essere tenuto in forma digitale, dopo ogni inserimento l'addetto autorizzato al trattamento deve effettuare una stampa in formato PDF, firmarla digitalmente e, successivamente, salvarla 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 garantiscono 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 registrate 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
- i supporti di backup
- la rete utilizzata per scaricare/visualizzare i dati dalle telecamere al server.
- 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. la protezione e 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. per 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;".

Il 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 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.

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.

3) Le informazioni di secondo livello sono facilmente accessibili per l'interessato e messi 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: "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 comporta 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 diritti di accesso e di portabilità dei dati?

Ai sensi dell'art. 15 del Regolamento (UE) relativo al diritto di accesso dell'interessato:

1. l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) 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;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) 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;

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento;

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi; se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune;

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

In ragione alla tipologia di trattamento che riguarda filmati l'interessato e di quanto disposto al punto 4 dell'art. 15 del Reg. (UE) 2016/679 l'interessato non può avere accesso ai filmati in forma integrale perché potrebbero contenere immagino di altri soggetti così violando i diritti e le libertà altrui. Ne consegue che in caso di esercizio del diritto di accesso con riferimento al punto 3 dell'articolo 15 dell'RGPD il titolare prima di fornire copia di quanto richiesto dovrà verificare che non siano presenti immagini relative ad altre persone e nel caso ne riscontri la presenza provvedere all'oscuramento delle immagini relative alle persone diverse dall'interessato.

Per l'esercizio del diritto di accesso, 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.

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.

Per quanto riguarda i trattamenti effettuati ai sensi del D.Lgs. 51/2018 il diritto di accesso è esercitabile ai sensi dell'art.11 del D.Lgs. 51/2018 non è previsto il diritto alla portabilità per i trattamenti effettuati ai sensi del D.Lgs. 51/2018.

Valutazione: Accettabile

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

Ai sensi dell'art. 16 GDPR l'interessato ha il diritto di ottenere la rettifica di dati personali inesatti ovvero l'integrazione di dati personali incompleti.

Considerati i tempi ristretti di conservazione dei dati e la tipologia di trattamento potrebbe essere impossibile procedere con l'esercizio di tali diritti.

Nel caso si verificano le condizioni per l'esercizio del diritto di rettifica, 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.

Ai sensi dell'art. 17 RGDP l'interessato ha il diritto alla cancellazione dei suoi dati: 1) nel caso che non siano più necessari rispetto alle finalità di raccolta; 2) nel caso si opponga al trattamento e non vi siano altri motivi legittimi per procedere con lo stesso; 3) nel caso i dati siano trattati illecitamente da parte del titolare del trattamento; 4) nel caso i dati debbano essere cancellati per adempiere ad un obbligo di legge cui è soggetto il titolare del trattamento. In tutti questi casi il titolare del trattamento dovrà procedere alla cancellazione di tali dati senza ingiustificato ritardo.

Non si applica il diritto alla cancellazione quando vi è un obbligo di legge da rispettare e/o un compito da svolgere nel pubblico interesse ovvero l'esercizio di pubblici poteri cui è investito il titolare del trattamento e non si applica per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria (art. 24 Cost.).

Per quanto riguarda i trattamenti effettuati ai sensi del D.Lgs. 51/2018 i diritti rettifica e cancellazione sono esercitabili ai sensi dell'art.12 del D.Lgs. 51/2018.

Valutazione: Accettabile

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

Ai sensi dell'art. 18 GDPR 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.

Ai sensi dell'art. 21 GDPR 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.

Per quanto riguarda i trattamenti effettuati ai sensi del D.Lgs. 51/2018 il diritto di limitazione è esercitabile ai sensi dell'art.14 del D.Lgs. 51/2018.

Valutazione: Accettabile

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

Nel caso si rilevi 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 (contrato) 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 è stata nominata Responsabile del trattamento la ditta che effettua la manutenzione all'impianto di videosorveglianza per quanto riguarda tutte le operazioni relative al trattamento dei dati ai fini manutentivi.

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

Crittografia

Non viene utilizzata la criptografia per la memorizzazione dei dati sul server.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

Implementare la criptografia delle immagini contenute sull'HD.

Commento di valutazione:

La criptografia dell'hard disk dove sono memorizzate le immagini ridurrebbe ulteriormente il rischio, nel caso di furto del server.

Controllo degli accessi logici

L'accesso e controllato da password di lunghezza minima di 8 caratteri composta da lettere, numeri e caratteri speciali.

Valutazione: Accettabile

Tracciabilità

Sono adottati appositi registri che documentano le operazioni di visualizzazione delle immagini, le operazioni di scarico delle immagini relative a fatti illeciti.

Valutazione: Accettabile

Archiviazione

I tempi di archiviazione sono limitati a 7 giorni, trascorso tale periodo i dati sono cancellati in modo irreversibile.

Valutazione: Accettabile

Minimizzazione dei dati

Il numero di persone identificate è ridotto in conseguenza al fatto che l'accesso alla visione delle immagini è limitato alle sole persone autorizzate formalmente al trattamento e in considerazione del fatto che essendo immagini è necessario procedere all'eventuale identificazione della persona e l'identificazione avviene solo nel caso sia rilevato un fatto illecito, i dati sono conservati per un periodo limitato.

Valutazione: Accettabile

Gestione postazioni

L'accesso alle immagini è limitato alle sole persone autorizzate formalmente al trattamento.

Per accedere alle postazioni è necessario essere fisicamente presenti all'interno del comune e l'accesso alle postazioni è protetto da login e password oppure attraverso sw di accesso remoto attivato dal personale interno solo per il periodo necessario

Valutazione: Accettabile

Manutenzione

Il sistema è affidato in manutenzione che è effettuata o recandosi sul posto o attraverso l'accesso al server dall'esterno attraverso sw di accesso remoto che viene attivato dal personale interno solo per il periodo necessario.

Valutazione: Accettabile

Contratto con il responsabile del trattamento

Il contratto con il responsabile del trattamento definisce puntualmente oggetto, durata, finalità del trattamento e obblighi delle parti contraenti.
In particolare, il contratto contiene, disposizioni relative a:

- gli obblighi dei responsabili in materia di riservatezza dei dati personali affidati;
- requisiti minimi di autenticazione degli utenti;
- clausole in materia di restituzione e/o distruzione dei dati allo scadere del contratto;
- regole per la gestione e la notifica di eventuali incidenti.

Valutazione: Accettabile

Sicurezza dei canali informatici

I canali informatici utilizzati sono canali sicuri che utilizzano protocolli che implementano la criptazione dei dati (wpa2-psk per autenticazione con User name e Password).

Valutazione: Accettabile

Controllo degli accessi fisici

La postazione per la visualizzazione delle immagini e collocata all'interno della sala di controllo dell'ufficio di Polizia Locale la stanza è chiusa a chiave e l'accesso alla sala è gestita dal responsabile dell'ufficio di Polizia Locale.

Valutazione: Accettabile

Sicurezza dell'hardware

La postazione per la visualizzazione delle immagini e collocata all'interno della sala di controllo dell'ufficio di Polizia Locale la stanza è chiusa a chiave e l'accesso alla sala è gestita dal responsabile dell'ufficio del Polizia Locale.

Valutazione: Accettabile

Protezione contro fonti di rischio non umane

La postazione per la visualizzazione delle immagini e collocata all'interno della sala di controllo dell'ufficio di Polizia Locale la stanza è chiusa a chiave e l'accesso alla sala è gestita dal responsabile dell'ufficio del Polizia Locale.

Valutazione: Accettabile

Politica di tutela della privacy

L'ufficio di Polizia locale ha implementato un'organizzazione interna idonea a garantire l'adeguatezza della protezione dei dati personali nominando e istruendo i soggetti interni autorizzati ad effettuare il trattamento dei dati personali.

Valutazione: Accettabile

Gestione delle politiche di tutela della privacy

L'ufficio di Polizia locale ha implementato una politica tesa a garantire l'adeguatezza della protezione dei dati personali nominando e istruendo i soggetti interni autorizzati ad effettuare il trattamento dei dati personali e nominando responsabili esterni al trattamento esclusivamente soggetti esterni che effettuano trattamenti per conto dell'ufficio di Polizia locale in grado di fornire adeguate garanzie di affidabilità.

Il titolare al momento dispone di un impianto documentale relativo alle misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.

Valutazione: Accettabile

Gestione dei rischi

Sul trattamento è stata effettuata la valutazione dei rischi per i diritti e per le libertà personali degli interessati (individuazione del trattamento di dati personali, dei dati trattati, dei supporti utilizzati, valutazione del rischio, definizione di misure esistenti o previste ecc.)

Valutazione: Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

È stata approvata una procedura e un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati.

Valutazione: Accettabile

Gestione del personale

Gli addetti al trattamento sono limitati nel numero, istruiti e responsabilizzati.

Valutazione: Accettabile

Vigilanza sulla protezione dei dati

Il DPO/RPD periodicamente effettua un audit finalizzato a verificare che siano correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali.

Il DPO/RDP effettua un'indagine tesa a consentirgli di avere una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il GDPR (verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità, ecc.).

Valutazione: Accettabile

Lotta contro il malware

Tutti i dispositivi utilizzati per accedere ai dati sono dotati di software antivirus mantenuti aggiornati.

Valutazione: Accettabile

Backup

Non viene effettuato il backup delle riprese video effettuate.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

Dotare il sistema di un sistema per il backup che abbia le stesse politiche di cancellazione di dati del sistema di videosorveglianza.

Commento di valutazione:

Il Backup dei dati ridurrebbe il rischio di perdita dei dati di registrazione in caso di danneggiamento dell'HD del server.

Si consideri che nello specifico la perdita dei danni andrebbe principalmente a danno del Comune e della collettività più che a danno dell'interessato inteso come soggetto che commette un eventuale illecito le cui immagini andrebbero perse in caso di danneggiamento dell'HD del server.

Prevenzione delle fonti di rischio

Il sistema è accessibile dall'esterno solo attraverso sw di accesso remoto che viene attivato dal personale interno solo per il periodo necessario.

Valutazione: Accettabile

Gestione del personale

Gli addetti al trattamento sono limitati nel numero, istruiti e responsabilizzati.

Valutazione: Accettabile

Gestione dei terzi che accedono ai dati

Il manutentore del sistema è contrattualizzato con clausole che garantiscono la riservatezza e il trattamento dei dati in sicurezza nei casi in cui sia chiamato ad intervenire.

Valutazione: Accettabile

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

Quali sono le principali minacce che potrebbero concretizzare il rischio?

malware, hacker, cancellazione involontaria, distruzione del dispositivo, furto del dispositivo, cancellazione volontaria

Quali sono le fonti di rischio?

Fonte umana esterna, Fonte non umana, Fonte umana interna

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

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

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

Limitata, considerata l'entità del rischio in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati in considerazione delle misure previste appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti.

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

Limitata, considerate le possibili fonti di rischio, le caratteristiche e livello di vulnerabilità del sistema, appare difficile che si concretizzino le minacce individuate.

Valutazione: Accettabile

Modifiche indesiderate dei dati

Quali sarebbero 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 consentire la concretizzazione del rischio?

hacker, malware, furto del dispositivo

Quali sono le fonti di rischio?

Fonte umana esterna, Fonte umana interna, Fonte non umana

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

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

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

Limitata, considerata l'entità del rischio in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati in considerazione delle misure previste appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti.

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

Limitata, considerate le possibili fonti di rischio, le caratteristiche e livello di vulnerabilità del sistema, appare difficile che si concretizzino le minacce individuate.

Valutazione: Accettabile

Perdita di dati

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

Non attribuzione di un illecito commesso

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

Furto del dispositivo, distruzione del dispositivo, cancellazione involontaria, hacker, malware

Quali sono le fonti di rischio?

Fonte non umana, Fonte umana esterna, Fonte umana interna

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

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

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

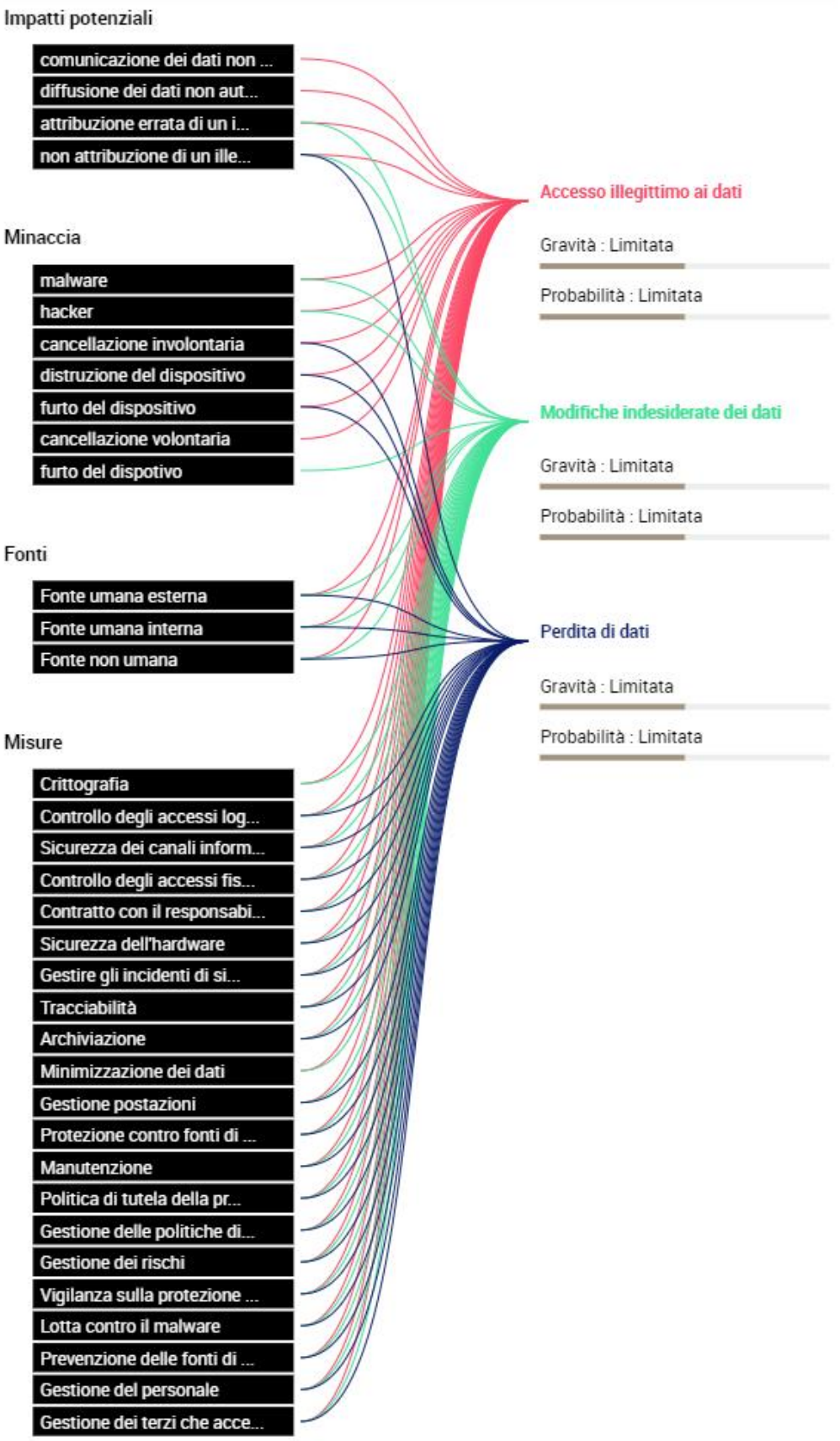
Limitata, considerata l'entità del rischio in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati in considerazione delle misure previste appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti.

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

Limitata, considerate le possibili fonti di rischio, le caratteristiche e livello di vulnerabilità del sistema, appare difficile che si concretizzino le minacce individuate.

Valutazione: Accettabile

Panoramica dei rischi



Data, 01 dicembre 2021

Approvazione della valutazione di impatto da parte del Titolare del trattamento

Il Sindaco

Giovanni PONCHIA

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

Il Responsabile della Protezione dei Dati Personali

Enrico Capirone