DATA PROTECTION IMPACT ASSESSMENT

Servizio di videosorveglianza

Vers. 0.1

PREMESSA METODOLOGICA

La presente valutazione di impatto è stata redatta assumendo quale indice generale l'Allegato 2 delle Linee Guida WP 248 rev.01, adattato alle esigenze specifiche del caso concreto.

La tassonomia relativa all'individuazione dei rischi, alle misure di contenimento, e alla loro misurazione è quella suggerita dal CNIL "Privacy Impact Assessment (Pia) – Knowledge Base.

Attenendosi al punto 1.5 di tale elaborato, si è quindi classificata la gravità dei rischi in:

1) Trascurabile
2) Limitato
3) Significativo
4) Massimo

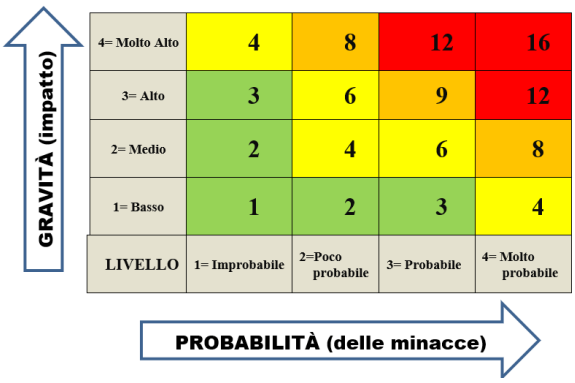
Assegnando un punteggio di 1 per Trascurabile, 2 per Limitato, 3 per Significativo e 4 per Massimo.

Anche la verosimiglianza (possibilità di accadimento) è stata classificata in:

1) Trascurabile
2) Limitato
3) Significativo
4) Massimo

Applicando a ciascuna voce il punteggio applicato per la gravità.

Il rischio inerente (o ponderato) è stato calcolato moltiplicando i due fattori G x V. Il risultato è stato confrontato con una matrice del rischio tratta dallo standard EN ISO 12100:2010



I valori compresi tra 1-3 sono stati ritenuti a basso rischio

I valori compresi tra 4-9 sono stati ritenuti a medio rischio – accettabile

I valori tra 10- 16 sono stati considerati ad alto rischio.

1. DESCRIZIONE SISTEMATICA DEL TRATTAMENTO

1.1 Natura, ambito di applicazione, contesto e finalità del trattamento

Il trattamento in oggetto è un sistema di videosorveglianza pubblica, per il controllo delle strade e del territorio comunale. Il sistema di videosorveglianza del Comune di Viareggio è progettato per monitorare e registrare attività all'interno di spazi pubblici, come piazze, strade e parchi, al fine di poter svolgere delle funzioni istituzionali dell'ente e in particolare controllare il flusso della viabilità sul territorio, supportare l'attività di rilevazione dei sinistri stradali, garantire maggior sicurezza pubblica e prevenire attività criminali, tutelare il patrimonio dell'ente, contrastare le attività di abbandono di rifiuti sul territorio comunale.

L'**ambito** di applicazione di questo trattamento deve intendersi come l'intero territorio del Comune di Viareggio e quindi potenzialmente può riguardare qualsiasi soggetto che si trovi a transitare su questo territorio. Sono state assunte iniziative al fine di limitare l'ampiezza di tale trattamento.

Il **contesto** del trattamento trova esplicazione nelle finalità per cui viene eseguito (che vedremo meglio in seguito) e riguarda la sicurezza delle strade, il controllo del traffico, il contrasto all'abbandono dei rifiuti, le indagini di polizia giudiziaria. Gli interessati sanno di poter essere oggetto del trattamento dati, sia per comune conoscenza sia per la presenza di cartellonistica specifica sul territorio stesso. Legittimamente si aspettano che i propri dati personali siano utilizzati per il perseguimento di una di queste finalità.

Le **finalità** del trattamento dati sono esplicitate dal regolamento Comunale, approvato con Delibera di Consiglio Comunale n. 23 del 20.04.2020, secondo cui "Le finalità istituzionali del suddetto impianto, conformi alle funzioni demandate al Comune di Viareggio, anche con riferimento al più ampio concetto di sicurezza urbana, così individuata secondo il D.M. dell'Interno 5 agosto 2008, sono finalizzati:

a) prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini;

b) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e a prevenire eventuali atti di vandalismo o danneggiamento del patrimonio pubblico;

c) rilevare situazioni di pericolo per la sicurezza pubblica, consentendo l'intervento degli operatori;

d) vigilanza del territorio al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, tutelando in tal modo coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un elevato grado di sicurezza nelle zone monitorate;

e) controllo dell'utilizzo di aree abusivamente impiegate come discariche di materiali o sostanze pericolose;

f) monitorare ai fini di sanzionare la violazione delle disposizioni dei vigenti Regolamenti Comunali per i servizi di smaltimento rifiuti e delle ordinanze emesse concernenti modalità, tipologia e orario di deposito dei rifiuti nonché del Regolamento per il decoro urbano, la cui violazione è sanzionata amministrativamente, laddove non sia risultato possibile o si sia rivelato non efficace il ricorso a strumenti e sistemi di controllo alternativi, quali l'espletamento di almeno 30 giorni dei previsti controlli e verifiche con proprio personale di Polizia Locale così come stabilito dal Garante sulla Privacy. Il sistema di videosorveglianza comporterà esclusivamente il trattamento dei dati personali, rilevati mediante le riprese televisive, e che in relazione ai luoghi di installazione delle videocamere, interesseranno i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.

g) monitorare l'attività di smaltimento dei rifiuti, contrastando l'abbandono di rifiuti sul territorio comunale e verificando le modalità di utilizzo delle strutture di conferimento.

Tipo di Dati Trattati

Il sistema di videosorveglianza raccoglie principalmente dati video e immagini fotografiche, che possono includere immagini di persone fisiche quali volti o caratteristiche fisiche, comportamenti e condotte, nonché immagini di autovetture e loro targhe. Da tali immagini sono estrapolate informazioni circa le persone che si trovano a transitare sul territorio comunale, le loro condotte, il loro adempimento a specifiche normative.

1.2 Destinatari del trattamento

I dati raccolti saranno trattati principalmente dal Titolare per perseguire le finalità sopra indicate. Potranno inoltre essere trasmessi a Forze di polizia o pubbliche Autorità incaricate di pubbliche funzioni qualora ciò sia necessario per l'adempimento di un obbligo di legge o di una pubblica funzione, a esempio lo svolgimento di indagini o gli accertamenti processuali. I dati quindi non sono destinati a uscire dal perimetro di sicurezza rappresentato da soggetti affidabili, tenuti a trattare i dati solo per finalità di pubblico interesse o di pubblici poteri e soggetti a stringenti vincoli di riservatezza.

1.3 Periodo di conservazione dei dati

Le immagini riprese dal sistema di videosorveglianza saranno conservate per un periodo massimo di dieci giorni, salvo l'esigenza specifica di impiegare tali immagini per il perseguimento delle finalità descritte (approfondimento di indagini, utilizzo delle immagini come prova, contestazione degli interessati, ecc.). Le informazioni tratte dalle immagini stesse potranno esser conservate per il tempo necessario all'espletamento delle funzioni indicate e per il perdurare delle procedure giudiziali o di sanzione, secondo le regole per la conservazione dei documenti.

1.4 Descrizione funzionale del Trattamento e ciclo vita dei dati

Il sistema di videosorveglianza pubblico utilizza telecamere di osservazione (sia di contesto che brandibili), telecamere per videosorveglianza dinamica (lettura targhe) e telecamere specifiche per il contrasto all'abbandono dei rifiuti (c.d. "fototrappole").

a) Telecamere di osservazione

Le telecamere di osservazione sono posizionate in luoghi pubblici per monitorare e registrare le attività in tempo reale ed in particolare sono posizionate nei seguenti luoghi:

VIAREGGIO
- piazza **Dante Alighieri intersezione via Mazzini**, carreggiate lato mare e lato monte: n. 4 telecamere fisse (collegamento radio);
- via **Battisti intersezione via Verdi**: n. 1 telecamera brandeggiante (collegamento fibra);
- via **Verdi zona piazza Cavour**: n. 1 telecamera brandeggiante (collegamento fibra);
- via **Battisti intersezione via Cavallotti**: n. 1 telecamera brandeggiante (collegamento fibra);
- via **Battisti intersezione via Machiavelli**: n. 1 telecamera brandeggiante (collegamento fibra);
- **Piazza M. Luisa**: n. 1 telecamera brandeggiante (collegamento fibra);
- viale **Marconi intersezione via Colombo**: n. 1 telecamera brandeggiante (collegamento fibra);
- viale **Marconi intersezione via Giusti:** n. 1 telecamera brandeggiante (collegamento fibra);
- viale **Marconi intersezione via Giotto**: n. 1 telecamera brandeggiante (collegamento fibra);
- viale **Marconi intersezione via Roma**: n. 1 telecamera brandeggiante (collegamento fibra);
- viale **Marconi intersezione via Gioia**: n. 1 telecamera brandeggiante (collegamento fibra);
- **piazza Mazzini**: n. 1 telecamera brandeggiante (collegamento fibra);
- viale **Margherita intersezione via San Martino**: n. 1 telecamera brandeggiante (collegamento fibra);
- viale **Margherita c/o piazza D'Azeglio** (edicola c/o Eden): n. 1 telecamera brandeggiante (collegamento fibra);

- viale **Margherita c/o piazza D'Azeglio** (c/o ex Odeon): n. 1 telecamera brandeggiante (collegamento radio);
- viale **Margherita intersezione via Zanardelli:** n. 1 telecamera brandeggiante (collegamento fibra);
- **Piazza Shelley**: n. 1 telecamera brandeggiante (collegamento radio);
- **via Bonaparte c/o la chiesa di San Paolino:** n. 2 telecamere (collegamento radio);
- viale **Europa c/o "Croce Verde**"; 1 telecamera 360 ° (collegamento radio);
- viale **Europa c/o locale "Corsaro Rosso**"; 1 telecamera 360 ° (collegamento radio);
- viale **Europa c/o "Ristorante Armanda**";1 telecamera 360 ° (collegamento radio);
- via dei **Pescatori intersezione via Petrarca**; 1 telecamera brandeggiante (collegamento radio);
- via **Coppino fronte piazzale Don Sirio Politi**: n. 1 telecamera brandeggiante (collegamento radio);
- via **Nicola Pisano intersezione via Savi**; 1 telecamera 360 ° (collegamento radio);
- via **Sant'Antonio c/o Torre Matilde**; 1 telecamera brandeggiante (collegamento radio);
- piazza **Santa Maria c/o Torre Matilde**; 1 telecamera 360 ° (collegamento radio);
- piazza **D'Azeglio intersezione via Garibaldi**; 1 telecamera 360 ° (collegamento radio);
- piazza **Nieri e Paolini c/o sede comunale**; 1 telecamera brandeggiante (collegamento radio);
- viale **Capponi intersezione via Vespucci**; 1 telecamera brandeggiante (collegamento radio);
- viale **Capponi intersezione via Marco Polo**; 1 telecamera brandeggiante (collegamento radio);
- via **Marco Polo intersezione viale Buonarroti**; 1 telecamera 360 ° (collegamento radio);
- via **Marco Polo intersezione via Maroncelli**; 1 telecamera 360 ° (collegamento radio);
- via **Aurelia Nord c/o rotonda via Marco Polo**; 1 telecamera 360 ° (collegamento radio);
- via **Aurelia c/o rotonda viale Einaudi:** n. 1 telecamera 360 ° (collegamento radio);
- via **Aurelia c/o rotonda Cittadella:** n. 1 telecamera 360 ° (collegamento radio);
- interno Pineta di Ponente c/o **Laghetto dei Cigni**: n. 1 telecamera 360 ° (collegamento radio),
- viale **rotonda Tobino/Pioppi (zona ex macelli)**: n. 1 telecamera brandeggiante (collegamento radio);
- via **Aurelia Sud intersezione via delle Darsene**: n. 1 telecamera brandeggiante (collegamento radio).

Frazione Torre del Lago:
- viale **Europa - Marina di Torre del Lago**:
viale europa "ex frau" telecamera brandeggiante (collegamento fibra);
viale europa "rotonda"telecamera brandeggiante (collegamento fibra);
viale europa " le tre scimmie telecamere brandeggiante (collegamento fibra);
viale europa "Boca Cica"telecamera brandeggiante (collegamento fibra);

- **stazione ferroviaria di Torre del Lago**: n. 1 telecamera brandeggiante (collegamento fibra) + n. 1 telecamera fissa (collegamento radio);
- via **Aurelia – Piazza del Popolo**: n. 1 telecamera 360 ° (collegamento fibra);
- viale **Puccini – Belvedere**: n. 1 telecamera brandeggiante (collegamento fibra);
- **piazza della Pace:** n.1 telecamera brandeggiante

Le immagini saranno trasmesse con collegamento in fibra ("wired") o con collegamento radio ("wireless") a un videoserver installato sui server del Comune e vengono storicizzate, per successive ed eventuali visualizzazioni, sui medesimi server.
Saranno visionabili da una sala video e da n. 4 postazioni di personal computer poste all'interno della sede del Comando della Polizia Municipale e da n. 1 postazione di personal computer distaccata presso la sez. Torre del Lago, tutte accessibili solo al personale autorizzato. Le registrazioni avvengono su supporti Hard Disk specifici TVCC.
Il collegamento wirless avviene con protocollo AES a 256 Bit.

Le immagini sono registrate con protocollo Hikvision e i dati sono oggetto di Backup, all'interno del sistema server, su supporti di registrazione Hard Disk paralleli in configurazione Raid.

Le immagini sono visionabili da una sala video e da n. 4 postazioni di personal computer poste all'interno della sede del Comando della Polizia Municipale e da n. 1 postazione di personal computer distaccata

presso la sez. Torre del Lago, a cui può avere accesso solo il personale del Comando di Polizia Municipale, appositamente formato ed incaricato.

In virtù del "Patto per la Sicurezza" siglato fra la Prefettura di Lucca e il Comune di Viareggio, è attiva la condivisione delle immagini con altre forze dell'ordine, sulla base di specifici accordi in via di definizione.

L'accesso alle immagini è regolato da un sistema AAA: è consentito previa autenticazione dell'utente mediante inserimento di nome utente e password (differenti per ciascuna persona abilitata a utilizzare la rete di videosorveglianza); ciascun utente avrà privilegi di accesso specifici che ricalchino le funzioni attribuite. L'accesso e le operazioni compiute sono registrate in un registro dei file di log.

La visione potrà avvenire "live" o per le immagini registrate, qualora ciò si renda necessario per le specifiche finalità.

Dopo dieci giorni le immagini saranno automaticamente sovrascritte, salvo che vi siano esigenze specifiche e concrete che richiedano la loro conservazione per periodi più lunghi.

L'installazione e la manutenzione del sistema sono affidati a un responsabile esterno che non può accedere ai dati personali salvo che per interventi di manutenzione.

b) Sorveglianza dinamica (lettura targhe)

Gli impianti di videosorveglianza dinamica (lettura targhe) sono posizionati:
- via **Aurelia intersezione via Garibaldi, fraz. Torre del Lago**: n. 1 telecamera direzione sud-nord (collegamento radio);
- viale **Tobino**: n. 2 telecamere direzione monti-mare (collegamento radio);
- via **Aurelia Nord**: n. 1 telecamera fronte campo sportivo direzione nord – sud (collegamento radio);
- via **dei Lecci c/o le Scuole della Tenuta** (collegamento radio);
- viale **Belluomini intersezione viale Einaudi**: n. 2 telecamere direzione nord-sud (collegamento radio).

Le modalità di trasmissione, conservazione e registrazione delle immagini avviene come indicato nel precedente punto a).

c) Sorveglianza sullo smaltimento dei rifiuti

L'impianto di videosorveglianza per il contrasto all'abbandono dei rifiuti e per sanzionare l'utilizzo non corretto delle strutture di conferimento avviene mediante un sistema di videocamere installate dal responsabile esterno, la società che gestisce lo smaltimento dei rifiuti. Le immagini sono trasmesse a un sub-Responsabile con competenze tecniche che provvede alla selezione delle immagini valide e pertinenti per l'individuazione dei soggetti che compiono azioni sanzionabili. Tali informazioni sono comunicate al Titolare del trattamento e nello specifico al Comando della Polizia Municipale. Il Responsabile esterno non ha alcuna visione delle immagini.

Le modalità di trasmissione, registrazione e comunicazione delle immagini sono le medesime di cui al punto a).

2. VALUTAZIONE DELLA NECESSITA' E DELLA PROPORZIONALITA' DEL TRATTAMENTO

2.1 Gli scopi del trattamento sono determinati, espliciti e legittimi?

Le finalità del trattamento sono previste da normativa nazionale e recepite dal Regolamento comunale sulla videosorveglianza. Sono esplicite e chiaramente delineate. L'intero sistema di videosorveglianza è stato progettato alla luce di tali finalità.

Queste possono sicuramente definirsi legittime poiché è lo stesso quadro normativo (come diremo nel punto successivo) a prevedere l'utilizzo degli strumenti di videosorveglianza fissandone le finalità.

2.2. Base Giuridica per il Trattamento

Il trattamento dei dati avviene innanzitutto ai sensi dell'art. 6, c.1, lett. e GDPR e in particolare perché 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. L'interesse pubblico o l'esercizio di pubblici poteri di cui in questione è attribuito dalla legge, da regolamenti o da atti amministrativi generali, così come esplicato dall'art. 2 ter c.1, d.l. 101/18.

In particolare si deve allora far riferimento all'art. 6, c.7. d.lgs 11/2009 in forza del quale "*Per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico*" ed all'art. 4 del D.L.14/2017 sulla sicurezza urbana secondo cui "*si intende per sicurezza urbana il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso [….] la prevenzione della criminalità, in particolare di tipo predatorio*".

È importante ricordare anche il dettato del d.lgs 152/06 in materia di contrasto all'abbandono dei rifiuti che conferisce funzioni ai comuni in merito a tali pratiche.

Altra base giuridica di liceità è poi il D.lgs. 51/2018 in materia di 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, nonchè alla libera circolazione di tali dati, che dunque regola i trattamenti effettuati per finalità di polizia giudiziaria.

L'insieme di queste norme rappresenta il fondamento essenziale per la liceità dei trattamenti in questione.

2.3 I dati trattati sono pertinenti, adeguati e limitati a quanto necessario?

La valutazione circa pertinenza, adeguatezza e necessità dei dati trattati non può che dare un esito positivo. E' ormai opinione ampiamente diffusa che la tutela della sicurezza urbana possa, in astratto, esser perseguita mediante il ricorso a strumenti di videosorveglianza. Questo è dimostrato sia dal dato normativo (che espressamente lo richiama), sia dall'uso che sempre più Forze dell'ordine ne fanno (anche attraverso la stipula di specifiche convenzioni o patti con gli enti locali) sia, da ultimo, dall'uso sempre più massiccio che ne è fatto.

Nel caso concreto si è operata una doppia valutazione. Quanto all'uso delle videocamere di osservazione si è ritenuto fossero indispensabili per un controllo di zone sensibili sul territorio comunale. Quanto alle videocamere installate per il controllo dei rifiuti si è potuto verificare che altre forme di controllo non invasive risultavano poco efficaci, anche in ragione dell'ampio numero di siti da verificare.

2.4. Qual è il periodo di conservazione dei dati?

Al riguardo dobbiamo distinguere il complesso delle immagini raccolte dal sistema di videosorveglianza, quelle selezionate perché significative al fine di perseguire le finalità stabilite, i dati tratti o dedotti dalle immagini.

Genericamente le immagini raccolte dai sistemi di videosorveglianza vengono sovrascritte di default dopo 10 (dieci) giorni. Tempi di conservazione più lunghi possono essere impostati qualora vi siano particolari

esigenze di indagini e non sia possibile soddisfarle in tale tempistica. Il prolungamento della conservazione, se motivato e indispensabile, rappresenta comunque un'eccezione.

Una volta individuate delle immagini necessarie per il perseguimento delle finalità indicate, queste e solo queste saranno conservate per tutto il tempo necessario all'espletamento delle attività connesse. A esempio in caso di accertamento di violazioni al Codice della Strada le immagini saranno conservate per i cinque anni successivi.

Le immagini utilizzate nei giudizi o in procedure giudiziarie saranno conservati sino al termine di tali procedure.

I dati tratti o dedotti dalle immagini (a esempio le targhe automobilistiche) saranno conservati per tutto il tempo necessario all'espletamento dei fini per cui sono usati.

2.5 Come sono informati del trattamento gli interessati?

Premesso che le tecniche di videosorveglianza nei centri urbani sono ampiamente note ai cittadini, si è scelto di informarli innanzitutto mediante l'apposizione degli appositi cartelli all'ingresso del territorio comunale.

Tale posizionamento ha dovuto contemperare le esigenze informative con quelle di rispetto ambientale con particolare riferimento all'"inquinamento da cartellonistica".

Si è poi provveduto a pubblicare l'informativa specifica ai sensi dell'art. 13 GDPR sul sito istituzionale del Comune.

2.6. Come fanno gli interessati a esercitare i loro diritti?

Gli interessati potranno esercitare i loro diritti scrivendo al Titolare, attraverso gli indirizzi forniti nell'ambito dell'informativa, oppure contattandolo mediante i canali istituzionali.

2.7. Come sono definiti e regolati gli obblighi dei responsabili del trattamento?

I rapporti con i responsabili del trattamento sono regolati attraverso un contratto e con uno specifico documento per la protezione dei dati, nel quale sono impartite le specifiche istruzioni.

2.8. Il trattamento prevede un trasferimento di dati al di fuori della comunità europea?

No, nessun trasferimento è previsto al di fuori della comunità europea.

3. Rischi

3.1 Misure esistenti o pianificate

3.1.1 Controllo degli accessi logici e tracciabilità

L'accesso ai dati avviene attraverso una postazione informatica dedicata dotata di username e password personale di accesso per ciascun operatore (unico e tracciabile).

Il software prevede la registrazione e conseguente tracciabilità degli accessi logici e delle operazioni effettuate dagli autorizzati al trattamento dei dati.

Assegnazione, a uso esclusivo, di una o più credenziali di autenticazione agli operatori.

Aggiornamento periodico delle credenziali di autenticazione.

3.1.2 Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dai dipendenti dell'ufficio in conformità a quanto previsto dalle procedure di riferimento, in maniera tale da garantire la riservatezza e la non visibilità a terzi non autorizzati. In particolare il loro trattamento e conservazione avvengono all'interno degli uffici della Polizia Municipale, luoghi sorvegliati e di difficile accesso per soggetti esterni non autorizzati.

3.1.3 Protezione contro il malware e vulnerabilità

Il sistema non prevede implementazioni di sicurezza in quanto tutta la rete, eccezione fatta per il cloud Targa System, non si connette a internet. In pratica è una rete privata chiusa su se stessa.

3.1.4 Crittografia

La crittografia avanzata è applicata alle informazioni che transitano dal server agli uffici competenti ratione materia della Polizia Locale.

3.1.5 Minimizzazione dei dati

Vengono raccolti e conservati unicamente i dati necessari e non sono richiesti dati eccedenti le finalità individuate.

3.1.6 Archiviazione e Backup

L'archiviazione dei dati personali trattati avviene in conformità alle procedure comunali di riferimento, garantendo la riservatezza e l'integrità dei dati personali trattati. Ogni dipendente, autorizzato al trattamento, è tenuto ad archiviare i documenti cartacei negli appositi raccoglitori e a conservare/salvare i documenti digitali sulle apposite apparecchiature in uso, protette da password di accesso.

Inoltre, le immagini rilevate dal sistema di VDS non sono oggetto di back-up all'interno del sistema server, su supporti di registrazione Hard Disk paralleli in configurazione Raid.

3.1.7 Controllo degli accessi fisici

- Gli accessi fisici agli uffici sono limitati e controllati dal personale della Polizia Municipale;
- l'accesso ai locali in cui sono visionati e conservati i dati avviene solo per personale espressamente autorizzato;
- la sala video è chiusa a chiave.

3.1.8 Sicurezza dell'hardware e prevenzione delle fonti di rischio

- Manutenzione programmata degli strumenti;
- Distruzione di tutti i supporti removibili non utilizzati;
- Estintori e loro revisione periodica;
- Accordo di assistenza continuativa con ditta di sicurezza informatica;
- Manutenzione costante impianti e apparecchiature elettriche ed elettroniche;
- Monitoraggio e impegno della direzione nel controllo delle regole in materia di salute e sicurezza sui luoghi di lavoro.

3.1.9 Manutenzione

- Manutenzione programmata degli strumenti
- Manutenzione costante impianti e apparecchiature elettriche ed elettroniche;
- Controllo sull'operato degli addetti alla manutenzione.

3.1.10 Sicurezza dei canali informatici

- La trasmissione dei dati avviene via radio in forma criptata con protocollo AES a 256 Bit mentre la registrazione delle immagini viene registrata con protocollo Hikvision

3.1.11 Politica di tutela della privacy

- Formazione sugli aspetti principali della Regolamento Europeo al momento dell'ingresso in servizio;
- Formazione periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione;
- Istruzioni agli incaricati, finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento senza l'ausilio di strumenti elettronici;
- Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durate le sessioni di lavoro;
- Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione;
- Istruzioni in merito all'accesso agli archivi digitali;
- Individuazione del profilo di autorizzazione anteriormente all'inizio del trattamento;
- Aggiornamento periodico o al verificarsi di eventuali modifiche della lista degli incaricati e dei profili di autorizzazione;
- Controllo degli accessi ai dati e programmi;
- Controllo sull'operato degli addetti alla manutenzione.

3.1.12 Misure di sicurezza specifiche

Ai sensi di quanto previsto dall'art. 24 del GDPR, i dati personali acquisiti mediante l'impiego dell'impianto VDS sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di qui al par. 2.1.1. del presente documento.
Ai sensi dell'art. 29 co. 2 della Direttiva UE 2016/680 il Titolare del trattamento, previa valutazione dei rischi mette in atto misure volte a:

- vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento ("controllo dell'accesso alle attrezzature");
- impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate ("controllo dei supporti di dati");
- impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione ("controllo della conservazione");
- impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati ("controllo dell'Utente") e garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali ci si riferisce la loro autorizzazione d'accesso ("controllo dell'accesso ai dati");
- garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione dei dati ("controllo della trasmissione");
- garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il moment della loro introduzione e la persona che la ha effettuata ("controllo dell'introduzione");
- impedire che i dati personali possano essere letti, copiati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati ("controllo del trasporto");
- garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati ("recupero");

- garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati (“affidabilità”) e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema (”integrità”).

3.2 Accesso illegittimo ai dati

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

Diffusione non autorizzata, intercettazione di informazioni in rete, pregiudizio alla reputazione. Il rischio principale in caso di diffusione non autorizzata è naturalmente la lesione del diritto alla riservatezza: dati inerenti la vita e la quotidianità degli interessati potrebbero esser diffusi verso soggetti non autorizzati. Si potrebbe poi dar luogo a una utilizzazione illecita di questi dati. Le immagini potrebbero essere utilizzate illegittimamente per attività di controllo dei lavoratori o per un loro utilizzo in cause di separazione o di divorzio.

3.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

Abuso di privilegi, accesso non autorizzato ai sistemi comunali per operazioni non consentite/non autorizzate, furto nei locali aziendali, vulnerabilità degli assets, azione di virus informatici o di programmi suscettibili di recare danno, distruzione totale o parziale e/o diffusione non autorizzata e/o inibizione dell'accesso ai dati, spamming o tecniche di sabotaggio.

3.2.3 Quali sono le fonti di rischio?

Fonti di rischio interne (dipendente infedele) ed esterne anche non umane come attacchi informatici, Virus e Malware.

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

Controllo degli accessi logici e tracciabilità; Sicurezza dei documenti cartacei; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Controllo degli accessi fisici; Manutenzione; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

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

In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi Trascurabile/Limitato con riferimento alla generalizzata diffusione dei dati. È invece da considerare SIGNIFICATIVO con riferimento al loro possibile utilizzo in giudizi o nell’ambito dei rapporti di lavoro.

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

Limitato. Le misure implementate rendono estremamente basso il rischio di accesso illegittimo da parte del personale interno, dotato peraltro di particolare affidabilità. Le cronache giudiziarie riferiscono però di episodi in cui pubblici ufficiali hanno acceduto illegittimamente a banche dati riservate passando le informazioni a soggetti interessati. Per questa ragione si è ritenuto di non applicare la categoria del “trascurabile” optando invece per Limitato.

Allo stesso modo si deve considerare Limitato il rischio di un accesso da esterno. Le misure applicate paiono essere adeguate a contenere il rischio. Inoltre si deve considerare che a oggi, stando alle cronache nazionali, non si sono verificati attacchi informatici ai danni di sistemi di videosorveglianza. Per questo si conferma la categoria di Limitato.

3.2.7 Come stimereste il rischio inerente o ponderato?

Il rischio inerente si configura come Medio – accettabile.

3.3 Modifiche indesiderate dei dati

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

Alterazione dei dati. Da questo potrebbero conseguire l'erogazione di sanzioni ingiuste, coinvolgimento in indagini giudiziali, una maggior difficoltà nel far valere dei diritti in un giudizio.

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

Errore informatico o errore umano. Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti, sottrazione di credenziali di autenticazione, accesso ai dati da parte di soggetti in orari non consentiti, errore umano, carenza di consapevolezza, disattenzione, incuria o indisponibilità, comportamenti contrari ai principi di sicurezza e protezione dei dati, comportamenti sleali o fraudolenti, operazioni accidentali non consentite e/o contrarie ai principi di sicurezza e protezione dei dati.

3.3.3 Quali sono le fonti di rischio?

Utenti interni e esterni all'organizzazione, attacchi informatici.

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

La possibilità di cancellare, modificare, cambiare parametri di sistema, visualizzare password o indirizzi di rete non viene abilitato a nessun utente, in modo da ridurre a zero il rischio di errori umani.

Oltre a queste misure si è previsto, in via generale: utilizzo di programmi costantemente aggiornati; Controllo degli accessi logici e tracciabilità; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Archiviazione e back-up; Controllo degli accessi fisici; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche, procedure di verifica dei risultati.

Si suggerisce comunque di prestare particolare attenzione da parte del personale al fine di garantire la sicurezza dell'ambiente informatico. Il personal computer infatti potrebbe essere oggetto di attacchi informatici generalizzati che vanno a colpire anche le immagini prodotte dalla video sorveglianza.

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

In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi Significativo.

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

Trascurabile.

Le misure individuate, pianificate ed adottate contribuiscono a mitigare i rischi individuati.

3.3.7 Come stimereste il rischio inerente o ponderato?

Il rischio inerente si configura come Basso.

3.4 Perdita di dati

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

Sotto il profilo dei diritti e delle libertà degli interessati, il rischio principale in caso di perdita o indisponibilità dei dati è rappresentato dalla perdita di prove utilizzabili in un eventuale ipotetico giudizio.

Non si configurano altri possibili rischi a carico degli interessati (semmai vi sarebbero rischi a carico dell'interesse pubblico che però esulano da questa analisi).

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

Errori umani nella gestione della sicurezza fisica, eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti a incuria, malfunzionamento, guasti, eventi naturali, alterazioni delle trasmissioni, indisponibilità o degrado degli strumenti, guasto ai sistemi complementari, sottrazione di strumenti contenenti dati, comportamenti sleali o fraudolenti, errore materiale, sottrazione di credenziali di autenticazione, azione di virus informatici o di programmi suscettibili di recare danno.

3.4.3 Quali sono le fonti di rischio?

Utenti esterni all'organizzazione, attacchi informatici, eventi calamitosi, malfunzionamenti.

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

La possibilità di cancellazione dei dati è preclusa al personale, in modo da ridurre le cancellazioni accidentali. Controllo degli accessi logici e tracciabilità; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Archiviazione e back-up; Controllo degli accessi fisici; Sicurezza dell'hardware e prevenzione delle fonti di rischio; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

Si suggerisce comunque di prestare particolare attenzione da parte del personale al fine di garantire la sicurezza dell'ambiente informatico. Il personal computer infatti potrebbe essere oggetto di attacchi informatici generalizzati che vanno a colpire anche le immagini prodotte dalla video sorveglianza.

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

In considerazione dei dati oggetto di trattamento e alla tassonomia adottata, il rischio individuato sarebbe da considerarsi Massimo. Questo perché espressamente è prevista la categoria delle prove giudiziali. In realtà si reputa che la tassonomia faccia riferimento alla perdita specifica di prove giudiziali già in possesso della parte. In questo caso ad andare perduta è la possibilità astratta che le immagini costituiscano una prova. Che i dati trattati contengano prove giudiziali è un'ipotesi meramente eventuale. Pertanto ad andare perduta non è la prova ma la possibilità di reperire un'eventuale prova (che potrebbe anche non sussistere). Per questa ragione si reputa che il rischio debba essere derubricato a SIGNIFICATIVO.

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

Limitato. Le misure individuate, pianificate ed adottate dovrebbero rendere poco probabile il verificarsi di un pericolo.

3.4.7 Come stimereste il rischio inerente o ponderato?

Il rischio inerente si configura come Medio - Accettabile.

4. Coinvolgimento delle parti interessate

4.1 Quale parere ha fornito il DPO in sede di consultazione?

Il Dpo ha espresso un parere positivo circa le misure adottate

4.2 Sono state raccolte le opinioni degli interessati?

Si è ritenuto non necessario raccogliere le opinioni degli interessati.

5. REVISIONE

La revisione è necessaria alla modifica delle condizioni di trattamento. In ogni caso è opportuna una revisione di verifica nel termine di due anni dall'adozione.