COMUNE DI CIVITAQUANA

PROVINCIA DI PESCARA

REGOLAMENTO PER LA DISCIPLINA DEL SISTEMA DI VIDEOSORVEGLIANZA

Approvato con Deliberazione del Consiglio Comunale n. 18 del 21/07/2023

INDICE

Art. 1 - Premessa

1. Il presente Regolamento disciplina le modalità di raccolta, trattamento e conservazione dei dati personali mediante sistemi di videosorveglianza gestiti dal Comune cui sono state conferite.

2. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, cioè che si realizza a distanza mediante dispositivi di ripresa video, captazione di immagini ed eventuale conseguente analisi, collegati a un centro di controllo e coordinamento direttamente gestito dal Servizio di Polizia Locale.

3. Le immagini, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi la videosorveglianza incide sul diritto fondamentale alla protezione dei dati personali riconosciuto alle persone fisiche dal diritto dell'Unione europea e dalla normativa vigente nazionale.

4. Con il presente Regolamento si garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti e impiegati dal Comune nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce, altresì, i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento, avuto riguardo anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico.

5. Ai fini delle definizioni di cui al presente Regolamento si deve fare riferimento al Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (di seguito GDPR), nonché al D. Lgs 30 giugno 2003, n. 196 (Codice della Privacy) così come modificato dal D. Lgs 10 agosto 2018, n. 101, e dall'art 2 del D. Lgs 18 maggio 2018, n. 51 relativo 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.

Art. 2 - Principi generali

1. Le norme del presente Regolamento si fondano sui principi di liceità, necessità, proporzionalità e finalità, come di seguito definiti.
Ai sensi dell'art. 6 del D.L. 23 febbraio 2009, n. 11, convertito nella Legge 23 aprile 2009, n. 38, *"per la tutela della sicurezza urbana i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico"*. Per sicurezza urbana (la cui definizione è stata da ultimo riformulata dal D.L. 14/2017, convertito nella Legge 18 aprile 2017 n. 48) si intende la tutela della sicurezza pubblica, intesa come attività di prevenzione e repressione dei reati, con esclusione delle funzioni di polizia amministrativa, nonché il bene pubblico che afferisce alla vivibilità e al decoro delle città. Gli impianti di videosorveglianza installati o in corso di realizzazione dal Comune attengono specificamente e in via principale alla tutela della sicurezza urbana e al presidio eventuale anche delle attività di polizia amministrativa.

2. Principio di liceità: 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 il Servizio di Polizia Locale sono investiti.

3. Principio di necessità: 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.

4. Principio di proporzionalità: 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.

5. Principio di finalità: gli scopi perseguiti devono essere determinati, espliciti e legittimi. è consentita la videosorveglianza come misura complementare volta a tutelare la sicurezza urbana anche nell'ambito di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o comunque con 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.

Art. 3 - Designato e autorizzati al trattamento

1. Titolare dei dati è il Comune di Civitaquana; designato al trattamento dei dati rilevati con apparecchi di videosorveglianza è il Responsabile del Servizio di Polizia locale, il quale può delegare in forma scritta le proprie funzioni. Egli vigila sull'utilizzo dei sistemi e sul trattamento delle immagini e dei dati in conformità agli scopi indicati nel presente Regolamento e alle altre disposizioni normative che disciplinano la materia.

2. Il Responsabile individua e nomina, con proprio provvedimento, nell'ambito degli appartenenti al Servizio di Polizia locale, gli autorizzati della gestione dell'impianto nel numero ritenuto sufficiente a garantire la corretta gestione del servizio di videosorveglianza.

3. Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.

ART. 4 - DPIA

1. Relativamente al trattamento dei dati di cui al presente regolamento è redatto il Documento di Valutazione di Impatto sulla Protezione Dati (noto anche come DPIA – Data Protection Impact Assesment) ai sensi dell'art. 35, comma 3, lettera c) del GDPR.

Art. 5 - Informativa

1. I soggetti interessati, che stanno per accedere o che si trovano in una zona videosorvegliata, devono essere informati mediante appositi cartelli conformi ai modelli approvati dall'Autorità Garante per la Protezione dei dati personali nei casi specificamente previsti dalla normativa.

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

3. Sul sito istituzionale del Comune di Civitaquana è inoltre pubblicata l'informativa concernente le modalità e le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal GDPR e dal D. Lgs. n. 51/2018 relativo 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.

Art. 6 - Finalità dei sistemi e architettura degli impianti

1. Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite al Comune di Civitaquana ai sensi dell'art. 6 del D.L. 23 febbraio 2009, n. 11, convertito con modificazioni dalla L. 23 aprile 2009, n. 38. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre forze di polizia, dovrà essere specificamente disciplinato con appositi accordi secondo la vigente normativa.

2. Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:

- attuazione di un sistema di sicurezza integrata ai sensi dell'art. 2 del dl 14/2017;
- tutela della sicurezza urbana nei luoghi pubblici o aperti al pubblico;
- tutela della sicurezza stradale, per monitorare la circolazione lungo le strade del territorio comunale e fornire ausilio in materia di polizia amministrativa in generale;
- tutela del patrimonio comunale, per presidiare gli accessi agli edifici comunali, dall'interno o dall'esterno e le aree adiacenti o pertinenti ad uffici od immobili comunali;
- tutela ambientale;
- all'esigenza, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali a norma del D. Lgs. n. 51/2018.

3. Il sistema di videosorveglianza implica il trattamento di dati personali che possono essere rilevati da telecamere tradizionali eventualmente munite di algoritmi di analisi video, metadatazione, conteggio delle persone e verifica dei comportamenti, o varchi lettura targhe connessi a blacklist in grado di verificare in tempo reale la regolarità di un transito di un veicolo.

4. Il Comune di Civitaquana promuove e attua, per la parte di competenza, politiche di controllo del territorio in collaborazione con gli altri Comuni della provincia e con i territori confinanti, con particolare riferimento al controllo dei veicoli in transito lungo i principali assi stradali di collegamento. A tal fine il Comune di Civitaquana potrebbe consentire l'utilizzo delle registrazioni degli impianti comunali di videosorveglianza, a condizioni di reciprocità e con le modalità di cui al comma 1.

5. Il Comune di Civitaquana promuove e attua, per la parte di competenza, politiche di controllo del territorio integrate con organi istituzionalmente preposti alla tutela della sicurezza e dell'ordine pubblico. A tal fine il Comune, previa intesa o su richiesta delle autorità di pubblica sicurezza o degli organi di polizia, può consentire l'utilizzo delle registrazioni video degli impianti comunali di videosorveglianza, con le modalità di cui al comma 1.

6. In caso di attivazione del centro operativo comunale (C.O.C.) le sole immagini in tempo reale rilevate dagli impianti attivi potranno essere messe a disposizione degli operatori del predetto C.O.C., debitamente autorizzati, per l'espletamento e lo svolgimento delle funzioni di Protezione Civile limitatamente alle emergenze in atto.

7. In presenza di aree o attività che risultino soggette a concreti pericoli, o per le quali ricorra una effettiva esigenza di deterrenza, e quando altre misure siano valutate insufficienti o inattuabili, il Comune di Civitaquana, per quanto di propria competenza, promuove il coinvolgimento dei privati per la realizzazione di singoli impianti di videosorveglianza, orientati comunque su aree o strade pubbliche o a uso pubblico, previa valutazione di idoneità dei siti e dei dispositivi; la valutazione sulla opportunità e necessità di tali installazioni verrà effettuata dal Comune nel rispetto dei principi di cui all'art. 2 del presente Regolamento, con particolare riferimento ai principi di necessità e proporzionalità. I privati interessati assumono su di sé ogni onere per acquistare le attrezzature e renderle operative, con connessione al sistema centrale, in conformità alle caratteristiche tecniche dell'impianto pubblico, le mettono a disposizione dell'Ente a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa. Il Comune assume su di sé gli oneri per la manutenzione periodica e la responsabilità della gestione dei dati raccolti.

8. Per tutti gli ambiti di nuova urbanizzazione, residenziale e non, soggetti a intervento diretto tramite PdC (Permesso di costruire) convenzionato o altro titolo edilizio, ove siano previste nuove strade classificate come pubbliche o come private a uso pubblico, in presenza di aree o attività che risultino soggette a concreti pericoli, o per le quali ricorra una effettiva esigenza di deterrenza, e quando altre misure siano valutate insufficienti o inattuabili, è d'obbligo per il soggetto attuatore assumere le spese e gli oneri per realizzare un sistema di videosorveglianza compatibile con l'impianto comunale, che sorvegli l'ingresso e l'uscita della strada. La valutazione sulla opportunità e necessità di tali installazioni verrà effettuata dal Comune nel rispetto dei principi di cui all'art. 2 del presente Regolamento, con particolare riferimento ai principi di necessità e proporzionalità. Tale sistema, una volta realizzato, può essere utilizzato e gestito esclusivamente dal Comune. Per tutte le procedure e le modalità di realizzazione, cessione d'uso e gestione si richiamano e si applicano integralmente le norme di cui al comma 7.

Art. 7 - Trattamento e conservazione dei dati

1. I dati personali oggetto di trattamento, effettuato con strumenti elettronici nel rispetto delle misure minime indicate dalla normativa relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per le finalità di cui al precedente art. 5, comma 2, e resi utilizzabili per operazioni compatibili con tali scopi;

c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;

d) conservati ordinariamente per un periodo non superiore ai 7 giorni successivi alla rilevazione, fatte salve speciali esigenze investigative di polizia giudiziaria con particolare riferimento ai varchi lettura targhe e ad altre esigenze correlate all'attività di istituto, comunque per il tempo strettamente necessario alla conclusione del relativo procedimento.

Art. 8 - Modalità di raccolta dei dati

1. I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di telecamere installate in luoghi pubblici ed aperti al pubblico, nonché in immobili di proprietà comunale, ubicati nel territorio di competenza.

2. Le telecamere di cui al precedente comma consentono riprese video a colori o in bianco e nero, possono essere dotate di brandeggio e di zoom ottico e sono collegate alla centrale operativa del Servizio di Polizia locale che potrà, esclusivamente per il perseguimento dei fini istituzionali, eventualmente digitalizzare o indicizzare le immagini.

3. I segnali video delle unità di ripresa sono visionabili presso la Centrale Operativa ubicata presso il Servizio di Polizia locale, sotto la responsabilità del Designato al trattamento dei dati.

4. Le immagini videoregistrate sono conservate per il periodo indicato all'art. 6, comma 1, lett. d), nella centrale di registrazione. Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione - ove tecnicamente possibile - mediante sovraregistrazione, con modalità tali da rendere non più utilizzabili i dati cancellati.

Art. 9 - Utilizzo di particolari sistemi mobili.

A) Dash Cam

1. I veicoli della Polizia locale possono essere dotati delle Dash Cam (telecamere a bordo veicoli di servizio) in conformità alle indicazioni e prescrizioni dettate in proposito dall'Autorità

Garante per la protezione dei dati personali, il cui trattamento dei dati è ricondotto nell'ambito del D. Lgs. n. 51/2018, trattandosi di *"dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela all'ordine e della sicurezza pubblica, nonché di polizia giudiziaria"*.
Il Responsabile del Servizio curerà la predisposizione di uno specifico disciplinare tecnico interno, da somministrare agli operatori di Polizia locale che saranno dotati dei predetti strumenti, con specificazione dei casi in cui le microcamere devono essere attivate, dei soggetti autorizzati a disporre l'attivazione, delle operazioni autorizzate nel caso di emergenza e di ogni altra misura organizzativa e tecnologica necessaria alla corretta e legittima gestione dei dispositivi e dei dati trattati.

2. Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare i principi di cui all'art. 5 del GDPR e richiamati all'art. 6 del presente Regolamento: in particolare i dati personali oggetto di trattamento devono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati.

B) Telecamere modulari e riposizionabili (foto trappole).

3. Il Servizio di Polizia locale può dotarsi di telecamere riposizionabili, anche del tipo foto-trappola, con generazione di allarmi da remoto per il monitoraggio attivo.

4. Le modalità di impiego dei dispositivi in questione saranno disciplinate con apposito provvedimento del Servizio di Polizia locale.

5. Gli apparati di videosorveglianza modulare riposizionabili vengono installati secondo necessità, nei luoghi teatro di illeciti penali; possono essere utilizzati per accertare illeciti amministrativi, solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D. Lgs. n. 51/2018 che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.

6. In ogni caso le modalità di trattamento e di conservazione dovranno rispettare quanto indicato dall'art. 6 del presente regolamento, nonché quanto disposto dalla vigente normativa.

C) Altri strumenti di videoripresa

7. Il Servizio di Polizia Locale, per lo svolgimento delle attività di competenza, può dotarsi di ogni altra tecnologia di ripresa video e di captazione di immagini necessaria al raggiungimento delle finalità istituzionali.

8. In particolare può dotarsi di Sistemi Aeromobili a Pilotaggio Remoto - droni - sia per l'esecuzione di riprese ai fini di tutela della sicurezza urbana, sia per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

9. In ogni caso, i dispositivi e il loro utilizzo devono essere conformi alla normativa vigente, con particolare riferimento alla regolamentazione adottata dall'Ente Nazionale per l'Aviazione Civile e al Codice della Navigazione.

10. Le modalità di impiego dei dispositivi in questione saranno disciplinate con apposito provvedimento del Servizio di Polizia Locale.

11. In ogni caso le modalità di trattamento e di conservazione dovranno rispettare quanto indicato dall'art. 6 del presente regolamento, nonché quanto disposto dalla vigente normativa.

Art. 10 - Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza ha diritto:

a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;

b) di essere informato sugli estremi identificativi del titolare e del designato al trattamento, oltre che sulle finalità e le modalità del trattamento dei dati;

c) di ottenere:

- la conferma dell'esistenza o meno di dati personali che lo riguardano;
- la trasmissione in forma intelligibile dei medesimi dati e della loro origine;
- l'informazione sulle procedure adottate in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

2. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, o per ragioni familiari meritevoli di protezione.

3. Le istanze sono presentate al Responsabile della protezione dati (RPD o DPO) dell'Ente, oppure al titolare o allo stesso Servizio di Polizia locale che, in tali casi, si faranno carico di informare e consultare il RPD/DPO.

Art. 11 - Accesso ai filmati.

1. Al di fuori dei diritti dell'interessato, di cui all'art. 9 del presente Regolamento, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente.

2. Ogni richiesta dovrà essere indirizzata al designato del trattamento dei dati di cui all'art. 3 del presente Regolamento.

3. Per finalità di indagine, l'Autorità giudiziaria e la Polizia giudiziaria possono acquisire copia delle riprese in formato digitale, formulando specifica richiesta scritta.

4. È consentito solo all'Autorità giudiziaria e alla Polizia giudiziaria di acquisire copia delle immagini. Non è consentito fornire direttamente ai cittadini copia delle immagini.

5. Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, i filmati possono essere richiesti ed acquisiti dall'organo di Polizia stradale che ha proceduto ai rilievi e in capo al quale è l'istruttoria relativa all'incidente.

6. Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'art. 391-quater c.p.p., può acquisire copia digitale dei filmati della videosorveglianza presentando specifica richiesta al designato del trattamento dei dati. In tal caso il difensore potrà presentare la richiesta motivata e provvedere alle spese per il rilascio di copia digitale dei filmati della videosorveglianza, riversato su apposito supporto. Salvo l'ipotesi di conservazione per diverse finalità, i dati si intendono disponibili per i normali tempi di conservazione.

7. Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al designato del trattamento che i filmati siano conservati oltre i termini di legge, per essere messi a disposizione dell'organo di polizia procedente. La richiesta deve comunque pervenire al Designato entro i termini di conservazione previsti. Spetterà all'organo di polizia in questione procedere a formale richiesta di acquisizione dei filmati. Tale richiesta dovrà comunque pervenire entro sessanta giorni dalla data dell'evento, decorsi i quali i dati non saranno ulteriormente conservati.

8. In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal designato del trattamento dei dati, dovrà annotare le operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, con lo scopo di garantire la genuinità dei dati stessi.

9. Possono essere divulgate immagini provenienti dagli impianti di videosorveglianza, previa anonimizzazione di ogni dato che consenta l'identificazione dei soggetti.

Art. 12 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati presso la centrale di registrazione individuata, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite dal Designato al trattamento dei dati.

2. In particolare l'accesso agli ambienti in cui è ubicata una postazione di controllo è consentito solamente al personale in servizio presso il Servizio di Polizia Locale autorizzato dal Responsabile e agli autorizzati. Possono essere autorizzati solo incaricati di servizi rientranti nei compiti istituzionali dell'Ente di appartenenza e per scopi connessi alle finalità di cui al presente regolamento, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, preventivamente individuato dal titolare o dal designato al trattamento.

3. Il Designato alla gestione e al trattamento impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.

4. Il Designato al trattamento designa e nomina i preposti in numero sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito degli operatori di Polizia locale.

5. I preposti andranno nominati tra gli Ufficiali ed Agenti in possesso della qualifica di agenti di Pubblica Sicurezza in servizio presso il Servizio di Polizia locale che per esperienza, capacità ed affidabilità, forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

6. La gestione e l'utilizzo dei sistemi di videosorveglianza aventi finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, è riservata agli organi di Polizia locale aventi qualifica di Ufficiali ed Agenti di Polizia giudiziaria ai sensi dell'art. 55 del codice di procedura penale.

7. Con l'atto di nomina, ai singoli preposti saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi in base alle differenti dislocazioni territoriali degli stessi.

8. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento.

9. Gli autorizzati al trattamento e i preposti saranno dotati di proprie credenziali di autenticazione di accesso al sistema.

10. Il sistema dovrà essere fornito di *"log"* di accesso, che saranno conservati per la durata di anni uno e soggetti a successiva modifica.

11. Sono garantite tutte le norme in materia di sicurezza del trattamento dei dati stabiliti dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Art. 13 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e dall'art 2 del D. Lgs. n.

51/2018 relativo 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.

Art. 14 — Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 77 e seguenti del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e dagli artt. 37 e seguenti del D. Lgs. n. 51/2018 relativo 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.

2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il Designato al trattamento dei dati personali, così come individuato dal precedente art. 6.

Art. 15 - Norma di rinvio

1. Per quanto non disciplinato dal presente Regolamento si rinvia al GDPR nonché al D. Lgs n. 196/2003 (Codice della Privacy), così come modificato dal D. Lgs. n. 101/2018 e dal D. Lgs. n. 51/2018 relativo 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 ai provvedimenti generali sulla videosorveglianza approvati dall'Autorità Garante per la Protezione dei dati personali, e alle indicazioni centrali dell'ANCI e del Ministero dell'Interno.

Al Responsabile del trattamento dei dati personali
inerenti impianti di videosorveglianza
Responsabile del Servizio di Polizia Locale
Comune di Civitaquana (PE)
Piazza Umberto I n. 26
65010 CIVITAQUANA
PEC: info@pec.comune.civitaquana.pe.it

RICHIESTA DI CONSERVAZIONE DELLE VIDEOREGISTRAZIONI DEGLI IMPIANTI DI VIDEOSORVEGLIANZA DEL COMUNE DI CIVITAQUANA

Il/la sottoscritto/a .. .., nato/a a... il...............................
residente a.. ... ...
in via...nr. civico. .... ,

PREMETTE

a di avere subito/assistito a quanto più oltre descritto, in spazi che presume essere ripresi dal sistema di videosorveglianza del Comune di Civitaquana:

____
____
____
____
____

- di essere consapevole che le immagini registrate vengono conservate per 7 giorni;

- di essere altresì consapevole che qualora entro i termini sopra indicati venga presentata al responsabile del trattamento motivata e dettagliata richiesta di accesso alle videoregistrazioni, per fatti costituenti ipotesi di reato, le immagini (ove reperite) possono essere acquisite per essere messe a disposizione dell'autorità giudiziaria e/o di polizia a seguito di presentazione di apposita denuncia;

- di essere altresì consapevole che le immagini estrapolate saranno conservate per una durata massima di 60 giorni al termine del quale, in assenza di richiesta prodotta dall'Autorità Giudiziaria e/o Organi di Polizia, saranno cancellate e distrutte;

- di essere consapevole, in relazione allo scopo sopra indicato, che le immagini, lasciate integre, vengano consegnate direttamente all'autorità giudiziaria e/o di polizia;

- di essere consapevole che si rende necessario indicare quale telecamera abbia potuto riprendere il fatto e che eventuali istanze generiche di conservazione di più filmati di telecamere sparse sul territorio comunale , e per la durata maggiore di 60 minuti, non saranno prese in considerazione, così come non potranno essere accolte le richieste di conservazione delle immagini di interi periodi temporali quali *"tutta la notte, tutta la mattina o tutto il pomeriggio",* senza circostanziare i tempi del fatto illecito presunto, e che tale istanza potrà essere accolta solo se formalizzata dall'Autorità Giudiziaria o dagli Organi di Polizia Giudiziaria che svolgono le attività investigative su ricezione di formale denuncia;

- di essere consapevole che la mancata allegazione del proprio documento d'identità alla presente costituisce l'irricevibilità dell'istanza e motivo ostativo di accoglimento ai sensi dell'art. 10 bis della L. 241/90;

Tutto ciò premesso il/la sottoscritto/a, a norma dell'art. 10 del Regolamento per la disciplina del sistema di videosorveglianza approvato con Deliberazione del Consiglio Comunale di Civitaquana nr. 18 del 21/07/2023

CHIEDE

di conservare le immagini rilevate dalle telecamere di videosorveglianza gestite dal comune di Civitaquana in:

Via/P.zza_________________________nr. civico_____dalle ore______alle ore______(massimo 60 minuti)

Via/P.zza_________________________nr. civico_____dalle ore______alle ore______(massimo 60 minuti)

Fornisce le seguenti informazioni utili:

1. luogo o luoghi di possibile ripresa ....

2. data ed orario di possibile ripresa ....
3. fascia oraria di possibile ripresa (massimo 60 minuti) dalle ore................................alle ore................................;
4. altre informazioni............... ....

Recapito (o contatto telefonico) per eventuali ulteriori approfondimenti

Mail...PEC...
In fede.

Civitaquana, lì........................ (firma)

Allega: - fotocopia di documento di riconoscimento

PETRUCCI EMILIO
DOTTORE COMMERCIALISTA-REVISORE CONTABILE

COMUNE DI CIVITAQUANA
PROVINCIA DI PESCARA
Piazza Umberto I°, 26

Il D.P.O.

L'anno 2023 il giorno 27 del mese di febbraio alle ore 18,30 si è riunito presso la Sede del Comune di Civitaquana il D.P.O., al fine di rilasciare parere circa il nuovo regolamento di videosorveglianza.

Occorre con l'occasione ricordare che un Comune deve porre in essere prima di installare qualsiasi impianto di videosorveglianza con foto camere, foto trappole e ogni altro strumento idoneo alla ripresa dei cittadini su aree pubbliche, ed in particolare abbiamo posto l'accento sull'importanza della valutazione di impatto.
La valutazione di impatto, (D.P.I.A., cioè Data Protection Impact Assessment nell'originale inglese) prevista dall'art. 35 del GDPR, è un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento ed il Titolare, ovvero il Comune che vuole installare l'impianto, deve svolgerla prima di piazzare anche solo una videocamera finta.
Si tratta di un procedimento complesso e non privo di dubbi, che non va confusa con la valutazione del rischio, che della DPIA costituisce una parte fondamentale, ma non unica, e che serve, in sostanza, per comprendere se e come i rischi insiti in qualsivoglia trattamento (e a maggior ragione insiti in un trattamento su larga scala e così invasivo come quello della video sorveglianza) possano avere impatti sui diritti e le libertà fondamentali degli interessati, secondo alcuni criteri: scoring, decisioni automatizzate, monitoraggio regolare e sistematico, categorie particolari di dati, trattamenti su larga scala, dataset correlati, dati relativi a soggetti vulnerabili, soluzioni tecnologiche innovative, trasferimenti extra UE, caratteristiche e identificabilità dell'interessato.
Con una corretta valutazione di impatto si assicura la trasparenza nel trattamento e la sicurezza dei dati, sia da un punto di vista tecnico sia organizzativo, nel rispetto del principio di accountability che permea l'intero regolamento privacy. Senza una DPIA correttamente svolta, ogni impianto di videosorveglianza è soggetto a sanzione e di conseguenza il Comune ed i suoi dirigenti a responsabilità.

I soggetti coinvolti

Montesilvano 65015-Via Danubio46/4
Tel 085/4452875
Fax 085/4452875

Teramo 65127- Via Luigi Brigiotti,12
Cell 328/2858260
Fax 085/4680637

mail:emilio_petrucci@virgilio.it
Pec : emilio.petrucci@odcecpescara.it
P.I. 02021510686

Dal punto di vista soggettivo, si occupano ed interessano della DPIA il Titolare, il DPO del Comune ed i Responsabili del trattamento, nonché gli amministratori di sistema, i soggetti installatori e chiunque abbia le competenze tecniche per "mettere le mani" nell'impianto di telecamere.
Il Titolare del trattamento è come sempre il soggetto richiamato alla responsabilità dal Regolamento. La sua partecipazione non è facoltativa, ma necessaria, pur se non sufficiente, per la redazione della DPIA. Che la rediga materialmente egli stesso (difficile) o che la deleghi a un dipendente o, più probabilmente, a un consulente esterno, il Titolare non può essere Ponzio Pilato e lavarsi le mani di quello che accade. Sarà lui, in caso di ispezione a dover dimostrare e illustrare le misure tecniche ed organizzative utilizzate, quindi sarà bene che le conosca.
Il Data Protection Officer, nel suo ruolo consultivo (art. 35 comma 2 del GDPR) e di sorveglianza del Regolamento (art 39 comma 1 lett. c) è chiamato dal Regolamento ad assistere il Titolare in questa procedura complessa. Attenzione: non è il DPO che redige la DPIA. Troppo spesso, infatti, si vedono Comuni che nominano un DPO lo "usano" come un consulente. Questo non è corretto dal punto di vista della accountability: il DPO verifica, controlla, dirige, indirizza e convalida, ma non può fare tutte queste cose se è lui stesso che ha redatto la DPIA, per un evidente problema di conflitto di interessi.
I responsabili del trattamento vanno coinvolti, in quanto l'impianto di videosorveglianza è certamente affidato ad una società esterna, che fornisce, installa e configura i dispositivi e pertanto non si può procedere senza di loro.
In alcuni casi può essere caldamente consigliata una richiesta di parere agli interessati, che in questo caso sono i cittadini: si tratta di un'ottima dimostrazione di accountability e i rapporti tra PA e cittadini potrebbero trarne giovamento (si badi però che quest'ultimo punto è meramente opzionale e facoltativo).

Importante inoltre è il rispetto, ad esempio, delle faq pubblicate il 5 dicembre 2020 sul sito del Garante privacy circa le domande più frequenti (FAQ) sui temi legati al **trattamento dei dati personali** nell'ambito dell'installazione di impianti di **videosorveglianza** da parte di soggetti pubblici e privati.

Pertanto, nel rispetto della normativa di legge generale e di settore, se ad esso conforme anche in fase applicativa, si rilascia parere favorevole.

Civitaquana, li 27/02/2023

Il D.P.O.
Dott. Emilio Petrucci

Montesilvano 65015-Via Danubio46/4
Tel 085/4452875
Fax 085/4452875
Teramo 65127- Via Luigi Brigiotti,12
Cell 328/2858260
Fax 085/4680637
mail:emilio_petrucci@virgilio.it
Pec : emilio.petrucci@odcecpescara.it
P.I. 02021510686

DPIA – Trattamento dati Videosorveglianza del Comune di Civitaquana

DPO e Titolare del trattamento/Referente

Nome del DPO/RPD

Petrucci Emilio

Parere del DPO/RPD

Trattamento implementabile in quanto conforme al GDPR 2016/679.

Richiesta del parere del Titolare del trattamento/Referente

È stato chiesto il parere del Titolare del trattamento e del Referente.

Nomi del Titolare del trattamento/Referente

Massimo Pasquariello

Posizione del Titolare del trattamento/Referente

Il trattamento può essere implementato.

Pareri del Titolare del trattamento/Referente

Trattamento implementabile in quanto conforme al GDPR 2016/679.

Nome autore
Rag. Adriano Doria per Actainfo srl

Data di creazione 05/06/2023

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Le operazioni di trattamento dati che il Comune di Civitaquana esegue sul territorio attraverso i diversi sistemi di videosorveglianza, perseguono le seguenti finalità:

- vigilanza sulla sicurezza stradale e della mobilità veicolare e pedonale;
- svolgimento di funzioni di pubblica sicurezza;
- vigilanza e prevenzione reati ed illeciti ambientali;
- attività di polizia giudiziaria.

L'attività di videosorveglianza eseguita dal Comune di Civitaquana è esercitata per lo svolgimento di funzioni e poteri pubblici ed il raggiungimento delle finalità istituzionali come sopra rappresentate e precisate, consentendo quindi di garantire ai cittadini il rispetto delle regole civili, penali ed amministrative nonché di civile educazione che consentono la normale convivenza e coabitazione nella condivisione di uno spirito di reciproco rispetto e di rispetto delle Istituzioni e delle loro funzioni.
I sistemi di videosorveglianza utilizzati dal Comune di Civitaquana sono, infatti, proporzionati ed efficaci rispetto alle finalità prefissate e sono tali da non comportare rischi ulteriori rispetto a quelli inseriti in un contesto di normale funzionalità dei sistemi tecnologici delle tipologie in uso.
Gli strumenti tecnologici in uso sono i seguenti:
1) sistema di videosorveglianza con telecamere fisse posizionate agli accessi all'area urbana e nel territorio, finalizzata al presidio del territorio stesso nonché alla vigilanza del traffico veicolare e pedonale in collaborazione con gli altri Comuni della provincia e con i territori confinanti, con particolare riferimento al controllo dei veicoli in transito lungo i principali assi stradali di collegamento, anche con dispositivi idonei alla lettura targhe;
2) sistema di videosorveglianza ambientale con "fototrappole" amovibili vengono installati secondo necessità, nei luoghi teatro di illeciti penali; possono essere utilizzati per accertare illeciti amministrativi, solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D. Lgs. n. 51/2018 che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.
3) I veicoli della Polizia locale possono essere dotati delle Dash Cam (telecamere a bordo veicoli di Servizio di Polizia Locale)

Quali sono le responsabilità connesse al trattamento?

Sono connesse al trattamento dei dati peronali le responsabilità del titolare del trattamento GDPR n. 2016/679 Articolo 24 - e ss.
Titolare del trattamento dei dati è il Comune di Civitaquana; designato al trattamento dei dati rilevati con apparecchi di videosorveglianza è il Responsabile del Servizio di Polizia Locale.
Egli vigila sul l'utilizzo dei sistemi e sul trattamento delle immagini e dei dati in conformità agli scopi indicati

nel Regolamento e alle altre disposizioni normative che disciplinano la materia.

Ci sono standard applicabili al trattamento?

Con riferimento al GDPR n. 2016/679, sono state emanate le "Linee Guida 3/2019 sul trattamento di dati personali attraverso Videosorveglianza", adottato dall'EDPB - Comitato dei Garanti Europei - in assemblea plenaria il 10 luglio 2019.
Nel novembre 2000 il Garante ha emanato delle linee guida contenenti gli indirizzi per garantire che l'installazione di dispositivi per la videosorveglianza rispetti le norme sulla privacy e sulla tutela della libertà delle persone, in particolare assicurando la proporzionalità tra mezzi impiegati e fini perseguiti. La materia è stata poi ulteriormente regolata da due provvedimenti generali del Garante, emanati rispettivamente nel 2004 e nel 2010, che contengono prescrizioni vincolanti per tutti i soggetti che intendono avvalersi di sistemi di videosorveglianza e precise garanzie per la privacy dei soggetti i cui dati vengano eventualmente raccolti e trattati tramite tali sistemi. Il provvedimento del 2010, in particolare, sostituisce il precedente e lo integra tenendo conto delle più recenti disposizioni normative in materia e delle possibilità offerte dalle nuove tecnologie. Una speciale attenzione è dedicata alle garanzie sul fronte dell'informazione ai soggetti che transitano in aree videosorvegliate (sempre obbligatori i cartelli informativi, salvo nel caso di telecamere installate a fini di sicurezza pubblica) e ai limiti per la conservazione dei dati raccolti tramite telecamere e videosorveglianza, che può superare le 24 ore solo in casi particolari (indagini di polizia e giudiziarie, sicurezza degli istituti di credito, ecc.). http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1002987

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati consistono in immagini e video registrati sul piano operativo; la registrazione è attiva sulle 24 ore e le immagini registrate vengono salvate solamente dal personale incaricato qualora vi sia una situazione di particolare criticità che necessita la documentazione video degli eventi.
Dati personali e giudiziari. Conservazione per la durata del procedimento.
Destinatari: Pubblica Amministrazione, Forze dell'ordine, cittadini.
Accesso ai dati consentito al Titolare, al DPO, al soggetto designato Responsabile del servizio di videosorveglianza ed ai soggetti, facenti parte del servizio, autorizzati al trattamento dei dati personali.

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

Il trattamento dei dati personali è effettuato a seguito dell'attivazione di tutti gli impianti/sistemi/presidi di video-sorveglianza installati sul territorio cittadino. La disponibilità tempestiva di immagini presso la Centrale Operativa ubicata presso il Servizio di Polizia Locale costituisce uno strumento di prevenzione e di razionalizzazione dell'azione delle pattuglie dislocate sul territorio comunale, anche in raccordo con altre Forze dell'ordine; attraverso tali strumenti l'Ente persegue l'intento di tutelare la popolazione ed il patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare. A tal fine il Comune, previa intesa o su richiesta della Autorità di Pubblica Sicurezza e degli Organi di Polizia, dispone l'utilizzo del sistema di video-sorveglianza in dotazione alla Polizia Locale, compresi i sistemi di lettura targhe e ZTL, ai fini di prevenzione e repressione di atti delittuosi anche nell'ambito del più ampio concetto di "sicurezza urbana", così individuata secondo il Decreto Ministro Interno 5 agosto 2008 decreto legge 20 febbraio 2017, n. 14 recante "Disposizioni urgenti in materia di sicurezza delle città" convertito con legge n. 48/2017. Tutto il sistema di video-sorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata. L'attività di video-sorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità succitate, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate alla normativa vigente in materia di "privacy" con un'apposita regolamentazione.

Quali sono le risorse di supporto ai dati?

Sistema di videosorveglianza urbana: le immagini vengono gestite direttamente dal videoregistratore che potrebbe essere collegato a un server NON collegato ad internet e vengono salvate su Hard Disk (SATA).
Fototrappole: le immagini vengono salvate a bordo della fototrappola su una SD-Card.
Dash Cam e Body Cam: è previsto l'utilizzo in futuro, ma al momento non sono attive.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

La liceità è data dall'art. 6 par. 1 del GDPR, in quanto "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 trattamento avviene altresì a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, ai sensi dell'art. 1 comma 2 del Dlgs 18 maggio 2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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".

Il Comune di Civitaquana, attraverso il Servizio di Polizia Locale, effettua il trattamento di dati personali mediante impianti di video-sorveglianza urbana, sia di osservazione che di contesto, ed altri sistemi di ripresa immagini di dati personali quali telecamere per lettura targhe, comprese quelle poste agli accessi della ZTL, scout camera (foto-trappole) e Street control; possono altresì essere previsti altri sistemi di video-sorveglianza. In particolare, l'uso di tutti i sistemi e tipologie di video-sorveglianza del territorio comunale è finalizzato a:

a) tutelare la sicurezza urbana di cui alla L. n. 38/2009 ss.mm.ii, Decreto del Ministro dell'interno del 05 agosto 2008 e decreto legge 20 febbraio 2017, n. 14 nonché secondo le modalità previste dal capitolo n. 5.1 del Provvedimento del Garante Privacy in materia di video-sorveglianza dd. 08/04/2010;

b) prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale secondo le modalità previste dal capitolo n. 5.1 del Provvedimento del Garante Privacy in materia di video-sorveglianza dd. 08/04/2010;

c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale ed a prevenire eventuali atti di vandalismo o danneggiamento;

d) controllare determinate aree e/o specifici siti comunali potenzialmente esposti a rischi di vandalismo o danneggiamento quali, a mero titolo esemplificativo, parchi, impianti sportivi e strutture ludico-ricreative;

e) al monitoraggio del traffico veicolare, al fine di prevenire o gestire problematiche inerenti la viabilità;

f) a tutelare in particolare coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un adeguato grado di sicurezza nelle zone anche per le finalità previste dal "Decreto sicurezza" approvato con Decreto Legge 23 febbraio 2009, n. 11 e convertito nella legge 23 aprile 2009, n. 38 (atti sessuali con minorenni, violenza sessuale di gruppo e atti persecutori);

g) controllare ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologia dei rifiuti scaricati ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, legge 24 novembre 1981, n. 689), secondo le previsioni di cui al capitolo n. 5.2 del Provvedimento del Garante Privacy in materia di video-sorveglianza dd. 08/04/2010;

h) prevenire eventuali atti di vandalismo e/o danneggiamento ovvero spaccio di sostanze stupefacenti presso Istituti scolastici in casi di stretta indispensabilità ed attivando gli impianti interni esclusivamente negli orari di chiusura degli Istituti secondo le modalità previste dal capitolo n. 4.3 del Provvedimento del Garante 4 Privacy in materia di video-sorveglianza dd. 08/04/2010;

i) supportare operazioni di protezione civile.

Quali sono le basi legali che rendono lecito il trattamento?

GDPR n. 2016/679 art. 6 e); L. 24.11.1981, n. 689; d.lg. 30.04.1992, n. 285 (art. 116); D.P.R. 16.12.1992, n. 495; d.lg. 18.08.2000, n. 267; Provvedimenti del Garante Privacy. Legge n. 179 del 30 novembre 2017; legge 6 novembre 2012, n. 190 art. 1, c. 51; art. 54-bis del decreto legislativo 30 marzo 2001, n. 165, art. 5 del Dlgs 18 maggio 2018, n. 51 e art. 23, comma 1, del d.P.R. n. 15 del 2018.

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 limitati e pertinenti alla finalità del servizio come previsto da art. 5 [GDPR].

I dati sono esatti e aggiornati?

I dati personali inesatti vengono rettificati o cancellati. La qualità dei dati è garantita dall'accesso limitato al personale autorizzato e istruito al trattamento dei dati personali derivanti dalla videosorveglianza.

Qual è il periodo di conservazione dei dati?

Il termine massimo di durata della conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di video- sorveglianza, fatte salve speciali esigenze di ulteriore conservazione" ai sensi del paragrafo 3.4.3 del provvedimento 08.04.2010 Garante Privacy. In relazione alle capacità di immagazzinamento dei dati forniti sui server, in condizioni di normale funzionamento le immagini riprese in tempo reale si sovrascrivono a quelle registrate, in piena osservanza della normativa vigente sulla privacy.

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

I soggetti sono informati con apposita cartellonistica approvata dalle Linee guida n. 3/2019 di EDPB riportante l'informativa ridotta ai sensi dell’art. 13 [GDPR].

Ove applicabile: come si ottiene il consenso degli interessati?

Poiché la liceità del trattamento è individuabile ex art. 6 par. 1 lett. E del GDPR, art. 5 del Dlgs 18 maggio 2018, n. 51 e art. 23, comma 1, del d.P.R. n. 15 del 2018 non necessita dell'ottenimento del consenso da parte degli interessati

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

In relazione al trattamento dei dati personali, è assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificarne le finalità, le modalità del trattamento e di ottenerne l'interruzione nel caso di utilizzo illecito, in particolare per la carenza dell'adozione delle idonee misure di sicurezza o per l'uso indebito da parte di soggetti non autorizzati. I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute, possono essere esercitati dagli eredi, da chi abbia un interesse proprio, da chi agisca a tutela dell'interessato o per ragioni familiari considerate particolarmente meritevoli di protezione.

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

Su presentazione di apposita istanza l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo tali dati personali in conformità con l'art. 17 del [GDPR]

Gli interessati sono messi in grado di esercitare i diritti di cui agli artt. 15 e seguenti?

Gli interessati possono esercitare i diritti di cui agli artt. 15 e seguenti rivolgendosi direttamente al Titolare o al Responsabile della Protezione Dati.
Nell'esercizio dei diritti dell'interessato può, anche conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.
Nel caso di esito negativo alle istanze di cui al presente articolo, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

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

Diritti esercitabili in sede di ricorso amministrativo o giudiziario.
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 in conformità con l'art. 21 del [GDPR]

Gli interessati sono messi in grado di esercitare i diritti di cui agli artt. 15 e seguenti?

Gli interessati possono esercitare i diritti di cui agli artt. 15 e seguenti rivolgendosi direttamente al Titolare o al Responsabile della Protezione Dati.
Nell'esercizio dei diritti dell'interessato può, anche conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.
Nel caso di esito negativo alle istanze di cui al presente articolo, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

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

Gli obblighi dei responsabili del trattamento sono disciplinati da una nomina avente natura contrattuale ai sensi dell’Art. 28 del [GDPR] e dal Regolamento sulla videosorveglianza approvato dal Consiglio comunale.

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

Non è previsto trasferimento dei dati extra UE

Rischi

Misure esistenti o pianificate

Crittografia

La trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni *wireless* (tecnologie Wi–Fi, Wi Max, Gprs).

Controllo degli accessi fisici

L’accesso alle centrali di controllo è consentito esclusivamente al titolare, ai designati ed agli autorizzati al trattamento.
Il controllo degli accessi viene eseguito dai soggetti designati e autorizzati appartenenti al Comando di Polizia Locale.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

1. Informare immediatamente il Titolare del trattamento dei dati personali (Sindaco) e il Responsabile del servizio.

2. Rimettere una relazione dettagliata al Titolare del trattamento dei dati personali.

3. Annotare l'evento sul Registro dei Data breach e redigere, ove necessario, il modulo di comunicazione al Garante con le informazioni relative all'evento utilizzando il modulo on line presente sul sito del Garante.

4. Se la violazione riguarda dati personali che limitano i diritti e le libertà delle persone fisiche, il titolare del Trattamento deve eseguire, entro 48/72 ore, la notifica al Garante.

5. Valutare, in base alla gravità, l'eventuale necessità di comunicazione della violazione all'interessato.

Procedura cartacea

Protezione fisica nell'accesso ai documenti e distruzione al termine della procedura.

Anonimizzazione

Non prevista

Partizionamento

Non previsto

Controllo degli accessi logici

Residente su procedura informatizzata con accesso controllato e riservato.

Tracciabilità

Nessuna

Archiviazione

Sul server locale fino a completamento della procedura.

Sicurezza dei documenti cartacei

In armadi chiusi con serratura, rispetto delle procedure previste nel manuale di conservazione.

Minimizzazione dei dati

Limitazione dei dati trattati a quelli indispensabili ai fini delle procedure attivate.

Vulnerabilità

Aggiornamento del software programmato, antivirus, firewall, autenticazione.
Limitazioni all'accesso fisico al materiale.

Lotta contro il malware

Livello di sicurezza e *antimalware* di sistema.

Gestione postazioni

Accesso riservato ai soggetti designati e autorizzati al trattamento dei dati.
Cifratura TLS dei flussi di dati, politica di rilascio dei cookie, audit di sicurezza.

Sicurezza dei siti web

Sistemi di sicurezza accesso e privacy.
Disciplinare generale di sicurezza, cifratura TLS dei flussi di dati, politica di rilascio dei cookie, audit di sicurezza.

Backup

Non previsto

Manutenzione

Servizio esterno con nomina a Responsabile del trattamento

Contratto con il responsabile del trattamento

Predisposta nomina, ex art. 28 GDPR 2016/679, per il Responsabile del trattamento che offre garanzie adeguate (in particolare quanto a conoscenze specialistiche, affidabilità e risorse).
Adottate misure (audit di sicurezza, visite agli impianti, ecc.) che consentono di assicurare l'effettività delle garanzie offerte dal Responsabile del trattamento in materia di protezione dei dati.

Sicurezza dei canali informatici

Sicurezza https, antivirus, firewall.

Sicurezza dell'hardware

Misure di inventariazione, compartimentalizzazione, ridondanza, limiti per l'accesso ecc. per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili ecc.) siano utilizzate per danneggiare i dati personali.

Prevenzione delle fonti di rischio

Formazione privacy dei soggetti designati e autorizzati al trattamento dei dati personali.

Esclusione del trasferimento dati al di fuori dell'UE

Protezione contro fonti di rischio non umane

Adottate misure preventive, di rilevamento, protezione, ecc. per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendi, danni provocati dall'acqua, incidenti interni o esterni, animali, ecc.) che potrebbero influire sulla sicurezza dei dati personali.

Politica di tutela della privacy

Nominare DPO, formare i soggetti designati e autorizzati, nominare responsabili del trattamento dei dati esterni secondo le disposizioni del GDPR 2016/679.

Gestione delle politiche di tutela della privacy

Attivato il Registro delle attività di trattamento e gestione degli adempimenti previsti dal GDPR.

Gestione dei rischi

Minimizzazione del trattamento *dei dati personali*, accesso controllato, valutazione del rischio dei trattamenti dei dati personali.

Integrare la protezione della privacy nei progetti

Applicazione dei principi di protezione dei dati personali by default e by design.

Valutazione DPO: Accettabile

Gestione del personale

Formazione e istruzioni GDPR dei soggetti autorizzati al trattamento dei dati personali.

Gestione dei terzi che accedono ai dati

Accesso con istanza da rivolgere al soggetto designato al trattamento che fisserà il giorno, l'ora ed il luogo dell'accesso.

Vigilanza sulla protezione dei dati

Audit periodici dello stato di protezione dei dati e della conformità con il GDPR per la verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità.

Rischi

Accesso illegittimo ai dati

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

Rischio di dispersione, Rischio di divulgazione

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Perdita documentazione

Quali sono le fonti di rischio?

Fonti umane interne, Virus e malware, eventi calamitosi

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Formazione ricorrente dei soggetti designati e autorizzati al trattamento dei dati personali. Controllo degli accessi fisici, Gestione delle politiche di tutela della privacy

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

Importante, Gravità del rischio importante

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

Limitata, Probabilità del rischio limitata

Rischi

Modifiche indesiderate dei dati

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

Sistema di videosorveglianza urbana: in caso di sottrazione delle immagini non si correrebbe alcun rischio in quanto le immagini sono soggette protezione con password e firma digitale.
Fototrappole: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

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

Sistema di videosorveglianza urbana: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità "logiche" ma esclusivamente fisiche dovute all'ingresso presso il Servizio di Polizia Locale, all'ingresso presso la Sala Macchine o presso un armadietto stradale.
Fototrappole: qualora la fototrappola venisse trafugata verrebbero perse anche le immagini salvate sulla SD-Card.

Quali sono le fonti di rischio?

Fonti umane interne, Eventi calamitosi, Attacchi informatici

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

I soggetti "autorizzati" a trattare i dati di videosorveglianza sono nominati con specifici atti, come da Regolamento Comunale, e sono istruiti e formati sul corretto trattamento.
Per l'accesso al Servizio di Polizia Locale di persone non dipendenti è permesso solo dopo l'identificazione e sono accolte da un dipendente del Servizio di Polizia Locale cui accede.
Molte delle funzionalità di controllo degli accessi possono essere abilitate o disabilitate in base alle esigenze o possono essere modificate per soddisfare un livello specifico di rischio. Le impostazioni predefinite per queste funzionalità di sicurezza sono state scelte per fornire un forte livello di sicurezza, pur mantenendo flessibilità e praticità.

In merito alle autorizzazioni:
Gestione granulare delle autorizzazioni basata sui ruoli.
Gestione delle autorizzazioni dell'applicazione (ad esempio, consentire a utenti specifici di utilizzare l'interfaccia basata sul Web).
Integrazione con i servizi directory per una gestione degli utenti semplificata e sicura.
In merito al controllo e reporting e di gestione degli utenti:
Registrazione dettagliata delle attività dell'amministratore e dell'utente a prova di manomissione.
Portale Web di amministrazione intuitivo per gestire utenti, autorizzazioni e ruoli.
In merito alla condivisione di dati:
Condivisione di prove all'interno ed esterne senza trasferimento di dati, duplicazione dei dati, supporti fisici o allegati e-mail.
Registrazione dettagliata della catena di custodia durante la condivisione.
Revocare l'accesso al contenuto condiviso in precedenza.
Impedire a un destinatario di contenuto condiviso di scaricare o ricondividere le prove.

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

Probabilità del rischio BASSO

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

Probabilità del rischio BASSO

Rischi

Perdita di dati

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

Sistema di videosorveglianza urbana: in caso di sottrazione delle immagini non si correrebbe alcun rischio in quanto le immagini sono soggette protezione con password e firma digitale.
Fototrappole: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

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

Attacchi informatici, Mancato rispetto delle procedure, Eventi calamitosi, Errore umano
Sistema di videosorveglianza urbana: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità "logiche" ma esclusivamente fisiche dovute all'ingresso presso il Servizio di Polizia Locale, all'ingresso presso la Sala Macchine o presso un armadietto stradale.
Fototrappole: qualora la fototrappola venisse trafugata verrebbero perse anche le immagini salvate sulla SD-Card.

Quali sono le fonti di rischio?

Fonti umane interne, Eventi calamitosi, Attacchi informatici

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

Controllo degli accessi fisici, Lotta contro il malware, Minimizzazione dei dati, Gestione delle politiche di tutela della privacy, Gestione dei terzi che accedono ai dati, Vigilanza sulla protezione dei dati

I soggetti "autorizzati" a trattare i dati di videosorveglianza sono nominati con specifici atti, come da Regolamento Comunale, e sono istruiti e formati sul corretto trattamento.
Per l'accesso al Servizio di Polizia Locale di persone non dipendenti è permesso solo dopo l'identificazione e sono accolte da un dipendente del Servizio di Polizia Locale cui accede.
Molte delle funzionalità di controllo degli accessi possono essere abilitate o disabilitate in base alle esigenze o possono essere modificate per soddisfare un livello specifico di rischio. Le impostazioni predefinite per queste funzionalità di sicurezza sono state scelte per fornire un forte livello di sicurezza, pur mantenendo flessibilità e praticità.
In merito alle autorizzazioni:
Gestione granulare delle autorizzazioni basata sui ruoli.
Gestione delle autorizzazioni dell'applicazione (ad esempio, consentire a utenti specifici di utilizzare l'interfaccia basata sul Web).
Integrazione con i servizi directory per una gestione degli utenti semplificata e sicura. In merito al controllo e reporting e di gestione degli utenti:
Registrazione dettagliata delle attività dell'amministratore e dell'utente a prova di manomissione. Portale Web di amministrazione intuitivo per gestire utenti, autorizzazioni e ruoli.
In merito alla condivisione di dati:
Condivisione di prove all'interno ed esterne senza trasferimento di dati, duplicazione dei dati, supporti fisici o allegati e-mail.
Registrazione dettagliata della catena di custodia durante la condivisione. Revocare l'accesso al contenuto condiviso in precedenza.
Impedire a un destinatario di contenuto condiviso di scaricare o ricondividere le prove.

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

Basso, Gravità del rischio **basso.**

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

Improbabile, Probabilità del rischio **improbabile**.

Integrità dei dati (alterazione, modifica)

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

Sistema di videosorveglianza urbana: le immagini sono soggette a protezione con password e firma digitale
Fototrappole: le immagini NON sono soggette a crittografazione.

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

Per poter modificare i video le persone che si volessero cimentare dovrebbero possedere una tecnologia molto avanzata.

Quali sono le fonti di rischio?

Sistema di videosorveglianza urbana: le fonti di rischio sono legate ad un accesso presso il Servizio di Polizia Locale, presso la sala Macchine o presso un armadio stradale.
Fototrappole: le fonti di rischio sono legate alla trafugazione dell'intera fototrappola con annessa SD-Card.

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

Per l'accesso al Servizio di Polizia Locale i soggetti non appartenenti allo stesso si muovono all'interno solo accompagnati e durante la notte viene presidiato e attivato l'allarme a tutela dell'immobile.

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

Il rischio viene valutato come Basso.

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

La stima individua l'evento come Improbabile.

Riservatezza dei dati (accesso abusivo, trattamento non conforme)

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

In caso di accesso illegittimo alle immagini si ritiene non si concretizzi un danno in quanto il soggetto prenderebbe semplicemente visione delle immagini registrate.

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

Accesso abusivo al server o accesso abusivo presso il Servizio di Polizia Locale.

Quali sono le fonti di rischio?

Accesso abusivo fisicamente in Servizio di Polizia Locale.

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

Per l'accesso al Servizio di Polizia Locale i soggetti non appartenenti allo stesso si muovono all'interno solo accompagnati e durante la notte viene presidiato e attivato l'allarme a tutela dell'immobile.

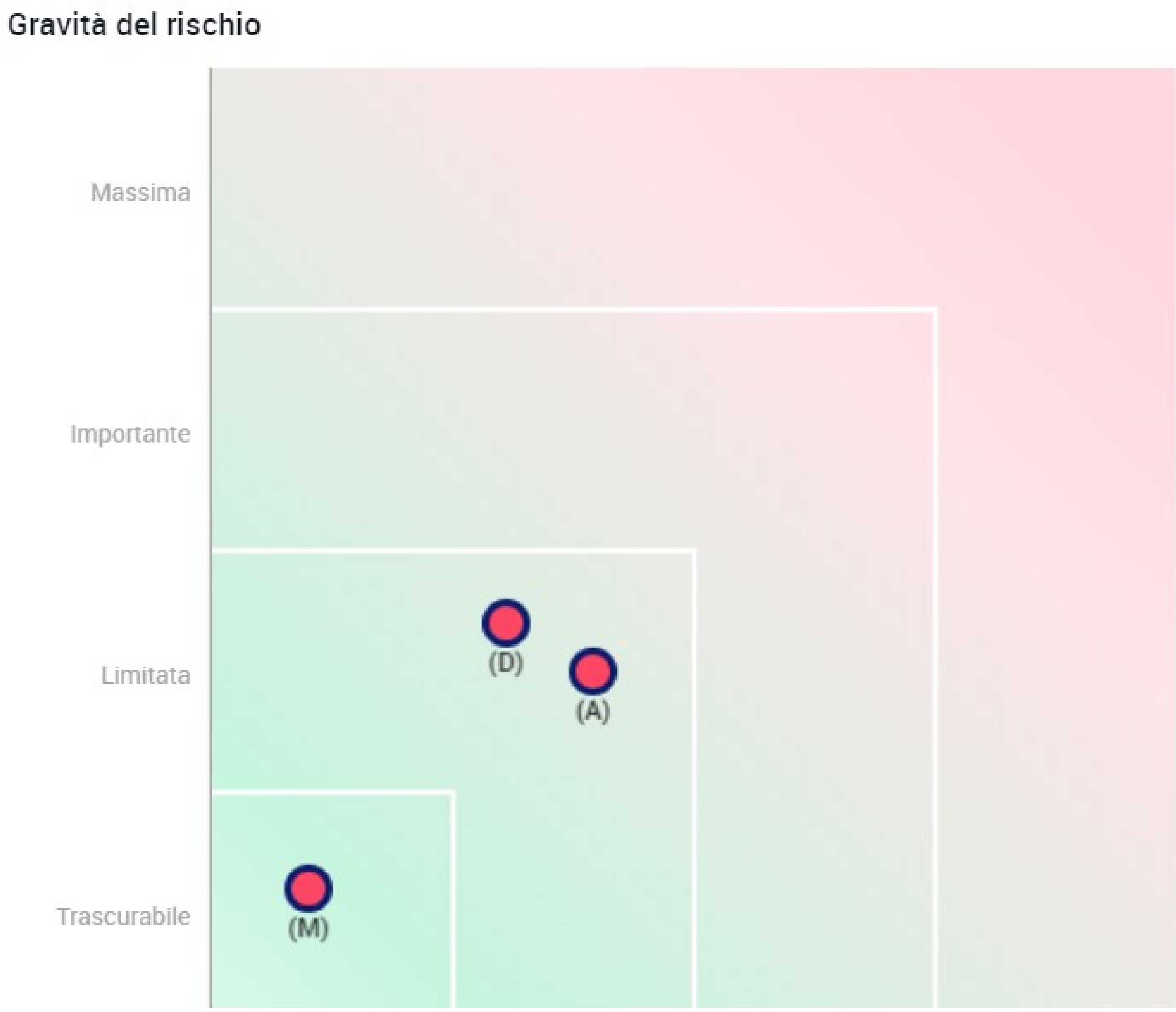
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Il rischio viene valutato come **Basso**.

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

La stima individua l'evento come **Improbabile**.

Mappatura dei rischi



Piano d'azione

Panoramica

Principi fondamentali

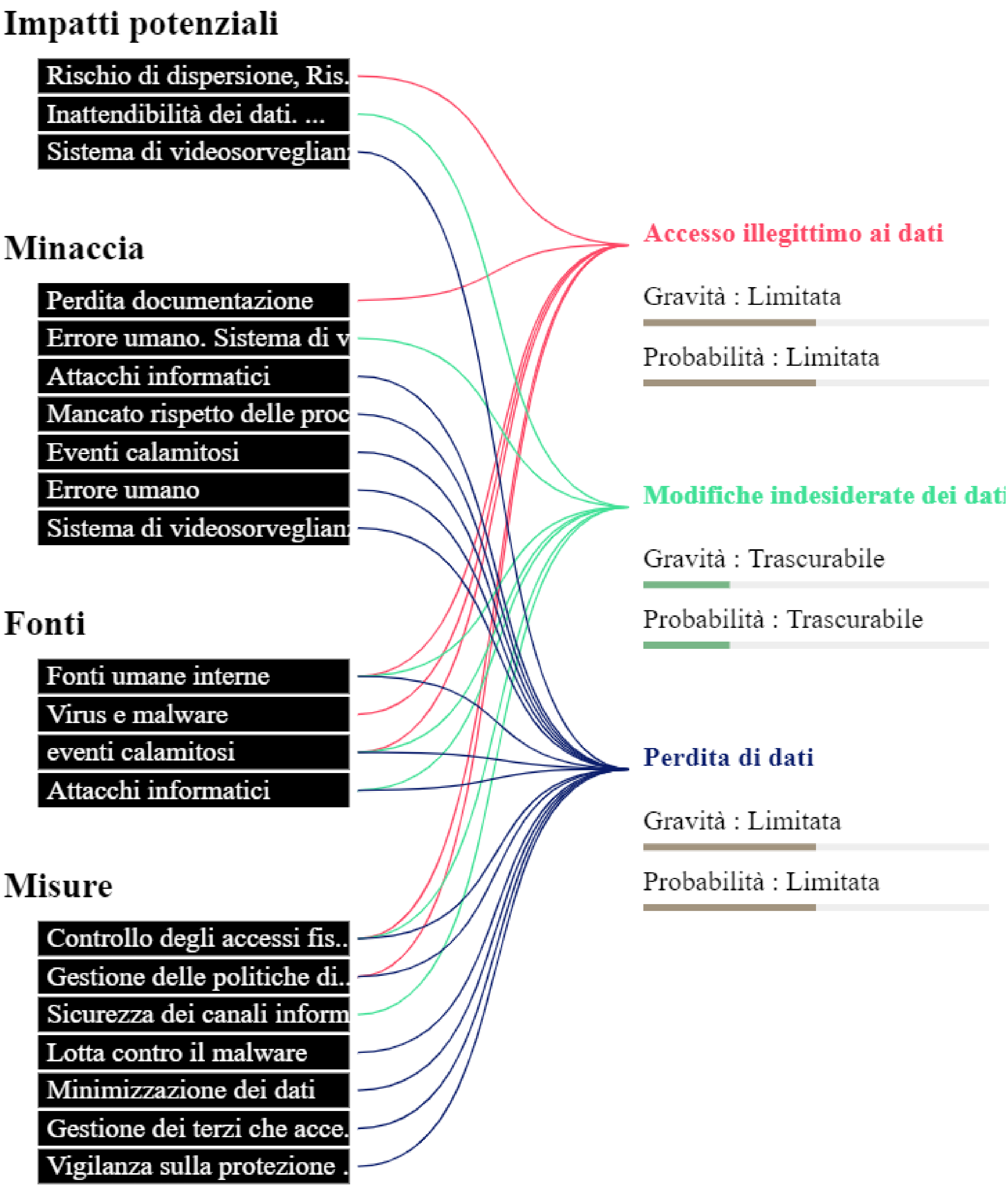
- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Diritto di accesso e diritto alla portabilità dei dati
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili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

Misure esistenti o pianificate

- Crittografia
- Controllo degli accessi fisici
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- Procedura cartacea
- Anonimizzazione
- Partizionamento
- Controllo degli accessi logici
- Tracciabilità
- Archiviazione
- Sicurezza dei documenti cartacei
- Minimizzazione dei dati
- Vulnerabilità
- Lotta contro il malware
- Gestione postazioni
- Sicurezza dei siti web
- Backup
- Manutenzione
- Contratto con il responsabile del trattamento
- Sicurezza dei canali informatici
- Sicurezza dell'hardware
- Prevenzione delle fonti di rischio
- Protezione contro fonti di rischio non umane
- Politica di tutela della privacy
- Gestione delle politiche di tutela della privacy
- Gestione dei rischi
- Integrare la protezione della privacy nei progetti
- Gestione del personale
- Gestione dei terzi che accedono ai dati

Rischi

Panoramica dei rischi



ALLEGATI:
- SCHEDA TECNICA VIDEOREGISTRATORE
- SCHEDA TECNICA TELECAMERE IN USO, ATTUALMENTE N. 15
- REGOLAMENTO PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA NEL TERRITORIO COMUNALE DI CIVITAQUANA
- NOMINA RESPONSABILE TRATTAMENTO DATI VIDEOSORVEGLIANZA

Firma Titolare del trattamento/Delegato

____