COMUNE DI MIAGLIANO
(Provincia di Biella)

REGOLAMENTO PER LA DISCIPLINA DEGLI IMPIANTI DI VIDEOSORVEGLIANZA SUL TERRITORIOCOMUNALE

Approvato con deliberazione di Consiglio Comunale n. 13 del 16.11.2023

Indice

CAPO I
PRINCIPI GENERALI

Art. 1 — Premessa

1. Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. La video sorveglianza incide sul diritto delle persone alla propria riservatezza.
2. Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di video sorveglianza gestiti ed impiegati dal Comune di Miagliano nel territorio comunale, 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.

Art. 2 - Principi generali

1. Le prescrizioni del presente Regolamento si fondano sui principi di liceità, necessità, proporzionalità e finalità.
2. Principio di liceità: il trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali ai sensi dell'art. 6.2 del Regolamento UE 679/2016 in materia di protezione dei dati personali.
3. Principio di necessità: il sistema di video sorveglianza è configurato 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 video sorveglianza 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 video sorveglianza possono essere attivati solo quando altre misure siano ponderatamente 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 deltrattamento.
5. Principio di finalità: gli scopi perseguiti devono essere determinati, espliciti e legittimi, in conformità alle indicazioni di cui al Provvedimento in materia di videosorveglianza – 8 aprile 2010 (G.U. n. 99 del 29 aprile 2010). E' consentita la video sorveglianza come misura complementare volta a migliorare la sicurezza all'interno del territorio comunale, sulla base di immagini utili in caso di fatti illeciti.

Art. 3 - Definizioni

1. Ai fini del presente Regolamento si intende:

a) per "banca di dati', il complesso di dati personali, formatosi presso la sala di controllo, e trattato esclusivamente mediante riprese televisive che, in relazione ai luoghi di installazione delle telecamere riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;

b) per il "trattamento", tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, l'eventuale diffusione, la cancellazione e la distribuzione di dati;

c) per "dato personale", qualunque informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di video sorveglianza;

d) per "titolare", il Comune di Miagliano nelle sue articolazioni interne, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;

e) per "responsabile", il soggetto che, per conto del Titolare, esegue attività di trattamento di dati personali;

f) per "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

g) per "interessato", la persona fisica a cui si riferiscono i dati personali;

h) per "comunicazione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

i) per "diffusione", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

j) per "dato anonimo", il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile

k) per "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;

l) per "GDPR" il Regolamento Europeo 670/2016;

m) per "Codice" il DLgs 196/2003 così come novellato dal DLgs 101/2018.

Art. 4 - Ambito di applicazione

1. Il presente Regolamento disciplina le modalità di raccolta, trattamento e conservazione di dati personali mediante sistemi di video sorveglianza attivati nel territorio urbano del Comune di Miagliano.

Art. 5 — Informativa

1. Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona video sorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa riportato in ALLEGATO al presente Regolamento.
2. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, è necessaria l'installazione di più cartelli.
3. L'informativa semplificata di cui ai punti precedenti rinvia ad un'informativa completa contenente tutti gli elementi previsti agli artt. 12, 13 e 14 del GDPR disponibile agevolmente agli interessati (sito internet, uffici comunali….).

Art. 6 - Finalità istituzionali dei sistemi di video sorveglianza

1. Le finalità perseguite mediante l'attivazione di sistemi di video sorveglianza sono del tutto conformi alle funzioni istituzionali attribuite al Comune di Miagliano dalle leggi, dallo Statuto e dai Regolamenti comunali vigenti.
2. Il trattamento dei dati personali è effettuato ai fini di:
    - monitorare la regolare circolazione lungo le strade comunali;
    - verificare le adiacenze di uffici comunali;
    - attivare misure di prevenzione e monitorare la sicurezza e di specifici siti comunali e del territorio;
    - controllare aree comunali oggetto di potenziale abbandono di rifiuti;
    - prevenire eventuali atti di vandalismo o danneggiamento agli immobili e al patrimonio comunale
3. Il sistema di video sorveglianza comporta il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti e veicoli che transitano nell'area interessata.
4. Il Comune promuove ed attua, per la parte di competenza, politiche di controllo del territorio, integrate con organi istituzionalmente preposti alla sicurezza pubblica.

A tal fine il Comune, previa intesa o su richiesta delle autorità di pubblica sicurezza e degli organi di polizia, può disporre l'utilizzo degli impianti comunali di video sorveglianza ai fini di prevenzione e repressione di atti delittuosi. I dati così raccolti vengono utilizzati esclusivamente dalle autorità ed organi anzidetti.

CAPO II
NOTIFICAZIONE, TRATTAMENTO E RACCOLTA DEI DATI

Art. 7 — Notificazione

In conformità all'art. 35, paragrafo 3, lettera c) del GDPR, il Titolare del Trattamento provvede ad effettuare apposita Valutazione di Impatto, consultando il Responsabile della Protezione dei Dati e in conformità a quanto previsto dall'art. 35, paragrafo 7 del GDPR. Periodicamente provvede al riesame della Valutazione di Impatto secondo quanto previsto dall' art. 35, paragrafo 11 del GDPR.

Art. 8 —Responsabile ed incaricati del trattamento

TITOLARE DEL TRATTAMENTO

Il Titolare del Trattamento dei dati è il Comune di Miagliano, al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.
Il Titolare del Trattamento tenuto conto della natura, del contesto e della finalità del trattamento, deve garantire, ed essere in grado di dimostrare, che il trattamento è effettuato non solo in maniera conforme alla normativa ma in maniera tale da non determinare rischi e quindi di non gravare sui diritti e le libertà degli interessati.

RESPONSABILE DEL TRATTAMENTO e INCARICATI/DESIGNATI DEL TRATTAMENTO *(art. 2 – quaterdecies Nuovo Codice Privacy – D.lgs 196/2003 aggiornato al D.lgs 101/2018)*

Il Responsabile del trattamento dei dati, nell'ambito del Comune di Miagliano, ai sensi della Legge, è individuato nella persona del Sindaco o suo delegato, nell'ambito delle funzioni attribuite dalle Leggi, Regolamenti e dalla Statuto.
Il Responsabile vigila sull'utilizzo dei sistemi e sul trattamento delle immagini e dei dati in conformità agli scopi del presente regolamento e alle altre disposizioni normative che disciplinano la materia ed in particolare alle eventuali disposizioni impartite dall'Autorità Garante per la protezione dei dati personali.
La responsabilità della gestione dell'impianto, il suo costante adeguamento alle norme di sicurezza in vigore e il costante controllo sull'uso delle immagini raccolte, spetta al Responsabile del trattamento dati della videosorveglianza.
Il Responsabile, designa e nomina quali preposti a garantire la gestione del servizio di videosorveglianza gli operatori degli Uffici Comunali competenti.
La gestione dell'impianto di videosorveglianza è riservata al Sindaco, e agli operatori degli Uffici Comunali competenti designati.
Con l'atto di nomina, ai singoli preposti saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi di vide sorveglianza.
In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, alle disposizioni della normativa vigente in materia di privacy e del presente regolamento.
Agli incaricati, designati, è affidata la custodia e conservazione delle password e/o delle chiavi di accesso ai sistemi, di eventuali armadi destinati alla conservazione dei supporti magnetici e simili.
Resta ferma la possibilità da parte delle Forze dell'Ordine e di Polizia, nell'esercizio delle loro funzioni di polizia, richiedere l'accesso ai sistemi di video sorveglianza.

RESPONSABILE ESTERNO

Ai sensi dell'art. 28 del GDPR, il Responsabile esterno del trattamento è la ditta affidataria responsabile dell'installazione della regolare manutenzione degli impianti di video sorveglianza del Comune di Miagliano.
I rapporti con il Responsabile esterno sono disciplinati da un contratto o da altro giuridico a norma del diritto dell'Unione o degli Stati membri.

Art. 9 — Trattamento e conservazione dei dati

Il trattamento dei dati personali oggetto della videosorveglianza deve avvenire tenendo conto dei principi a norma dell'art. 5 del GDPR, ossia "liceità, correttezza e trasparenza, minimizzazione dei dati, limitazione delle finalità, esattezza, limitazione della conservazione, integrità e riservatezza" e nello specifico:
a) i dati devono essere trattati in modo lecito e secondo correttezza;
b) i dati devono essere raccolti e registrati per le finalità di cui al presente regolamento, e resi utilizzabili per operazioni compatibili con tali scopi;
c) i dati devono essere raccolti in modo pertinente completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
d) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
e) i dati devono essere conservati per un periodo non superiore ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o servizi, nonché nel caso in cui si debba adire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Inoltre soltanto nel caso in cui nell'arco dei sette giorni di conservazione delle registrazioni pervengano segnalazioni di furti, atti di vandalismo e/o atti similari o comunque di danni per il patrimonio comunale e/o pubblico, le immagini devono essere conservate per essere messe a disposizione dell'autorità di polizia o dell'autorità giudiziaria;
f) L'eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta all'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

Art. 10— Modalità di raccolta dei dati

I dati personali sono ripresi attraverso le telecamere dell'impianto di video sorveglianza comunale (e depositati nei relativi hardware e software), anche attraverso foto-trappole e/o altri strumenti elettronici che si rendessero necessari e comunque conformi al dettato del presente regolamento.

Le telecamere dei sistemi di video sorveglianza sono installate in corrispondenza dei principali svincoli, incroci, piazze, immobili di proprietà comunale ubicati nel territorio urbano e consentono riprese video in bianco/nero o a colori, e possono essere dotate di zoom ottico programmati.

Presso la sede comunale, nel luogo all'uopo preposto, è installato il server di gestione dedicato e la strumentazione necessaria per il corretto funzionamento del sistema di video sorveglianza nonchè i monitor di controllo per la visione diretta.

Le immagini videoregistrate sono conservate per il periodo indicato all'art. 9, presso i locali nella sede comunale. Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione, anche eventualmente mediante sovraregistrazione, con modalità tali da rendere non utilizzabili i dati cancellati.

Art. 11 - Obblighi degli operatori

1. L'utilizzo delle telecamere è consentito solo per la sorveglianza di quanto si svolge nelle aree pubbliche.
2. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità e per l'esclusivo perseguimento delle finalità di cui al presente regolamento.
3. La mancata osservanza degli obblighi di cui al presente articolo comporterà l'applicazione di sanzioni disciplinari ed amministrative, e, ove previsto dalla vigente normativa, l'avvio degli eventuali procedimenti penali.

CAPO III

DIRITTI, SICUREZZA E LIMITI NEL TRATTAMENTO DEI DATI

Art. 12 - Diritti dell'interessato

1) I diritti che l'interessato può esercitare sono quelli previsti dagli Artt. 15, 16, 17, 18, 19, 21, 22 del GDPR.
2) L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, la loro comunicazione in forma intelligibile e la possibilità di effettuare reclamo presso l'Autorità di controllo.
3) L'interessato ha diritto di ottenere l'indicazione:

a. dell'origine dei dati personali;
b. delle finalità e modalità del trattamento;
c. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d. degli estremi identificativi del Titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2 del GDPR;
e. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati/addetti.

4) L'interessato ha diritto di ottenere:

a. l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b. 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;

c. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

5) L'interessato ha diritto di opporsi, in tutto o in parte, per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Art. 13 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
   a) distrutti;
   b) trasferiti all'autorità di Polizia di Stato (o altri organi di Polizia) purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
   c) conservati per fini esclusivamente istituzionali.

La cessione dei dati in violazione di quanto previsto dal comma precedente lett. b) o di altre disposizioni di legge in materia di trattamento dei dati personali determina la loro inutilizzabilità, fatta salva l'applicazione di sanzioni disciplinari ed amministrative, e, ove previsto dalla vigente normativa l'avvio degli eventuali procedimenti penali.

Art. 14 - Danni cagionati per effetto del trattamento di dati personali

1) Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile esterno ai sensi delle disposizioni di cui all'art. 82 dell'GDPR.

2) Il Titolare o il Responsabile esterno del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

3) Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'art. 79, paragrafo 2 dell'GDPR.

CAPO IV

TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 15 — Tutela

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss. dell'GDPR ed alle previsioni del D.Lgs. 196/2003 e ss.mm.ii.

CAPO V

NORME FINALI

Art. 16 — Norma di rinvio

Per quanto non disciplinato dal presente Regolamento si rinvia al GDPR 2016/679, al DLgs 196/2003 così come novellato dal DLgs 101/2018 e comunque reperire tutte le informazioni su www.garanteprivacy.it

.

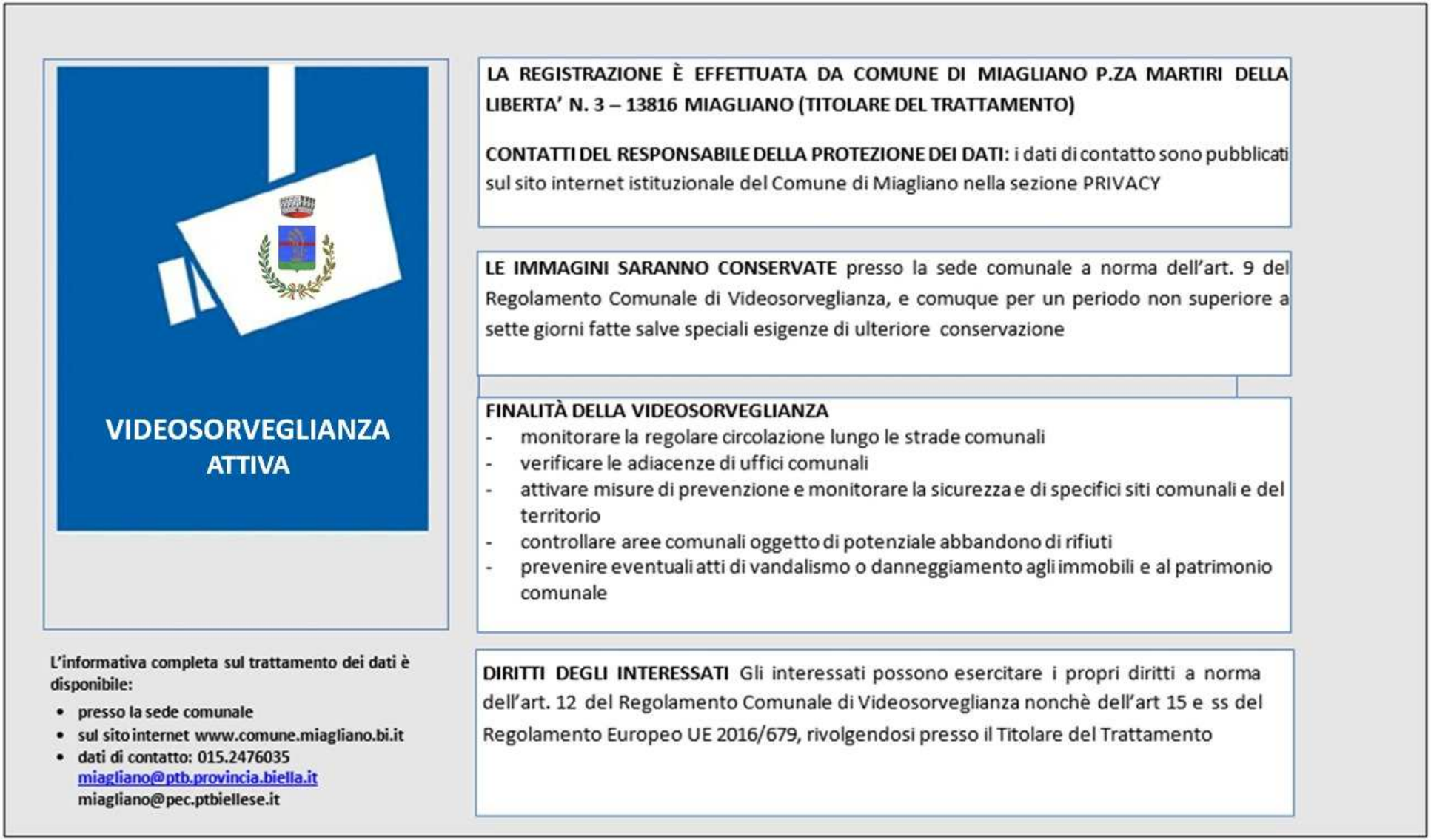
Art. 17 - Pubblicità del Regolamento

Copia del presente Regolamento, a norma dell'art. 22 della legge 7 agosto 1990, n. 241, e successive modificazioni ed integrazioni, sarà tenuta a disposizione del pubblico perché ne possa prendere visione in qualsiasi momento.
Copia dello stesso sarà altresì pubblicata sul sito internet del Comune, nella sezione Regolamenti e Amministrazione Trasparente.

Art. 18 - Entrata in vigore

1. Il presente Regolamento, dopo l'acquisita esecutività della deliberazione del Consiglio comunale che lo approva, è pubblicato per quindici giorni all'Albo pretorio ed entra in vigore il giorno successivo all'ultimo di pubblicazione.
2. Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.

Allegato – Modello semplificato cartello videosorveglianza



Originale

COMUNE DI MIAGLIANO

PROVINCIA DI BIELLA

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE N.54

OGGETTO:

Valutazione d'impatto sulla protezione dei dati (DPIA) - impianto di videosorveglianza ex Reg. Comunale n. 13 del 16/11/2023

L'anno duemilaventiquattro addì diciotto del mese di dicembre alle ore diciannove e minuti cinquanta nella solita sala delle adunanze, previa l'osservanza di tutte le formalità prescritte dalla vigente normativa, vennero per oggi convocati i componenti di questa Giunta Comunale, nelle persone dei Signori:

Cognome e Nome	Presente
1. MOGNAZ Alessandro - Sindaco	Sì
2. VINETTI Mauro - Assessore	Sì
3. BALDI CINZIA - Assessore	Sì
Totale Presenti:	3
Totale Assenti:	0

Con l'intervento e l'opera del Segretario Comunale Signora DURIO Dr.ssa Carmen la quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti il Sig. MOGNAZ Alessandro assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

Oggetto: Valutazione d'impatto sulla protezione dei dati (DPIA) - impianto di videosorveglianza ex Reg. Comunale n. 13 del 16/11/2023

Il Sindaco

Preso atto che:

- In data 27 aprile 2016, il Parlamento Europeo ed il Consiglio Europeo hanno approvato il Regolamento UE 2016/679 (GDPR- General Data Protection Regulation), relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Il Regolamento UE, pubblicato il 4 maggio 2016 nella Gazzetta Ufficiale dell'Unione Europea (GUUE), abroga la direttiva 95/46/CE e mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione Europea;
- Il Regolamento è diventato definitivamente e direttamente applicabile in tutti i Paesi UE, a partire dal 25 maggio 2018;
- Il Garante per la protezione dei dati personali ha pubblicato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, la quale ha la funzione di illustrare un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, dovranno tenere presenti in vista della piena applicazione del Regolamento;
- Ai sensi dell'art. 13 della Legge n.163/2017, il Governo è stato delegato ad adottare, entro sei mesi dalla entrata in vigore del Regolamento europeo, uno o più decreti legislativi al fine di adeguarvi il quadro normativo;

Rilevato che:

- Le norme introdotte dal Regolamento UE 2016/679 consistono in obblighi organizzativi, documentali e tecnici, che tutti i Titolari del trattamento dei dati personali devono, fin da subito, rispettare per garantire, entro il 25 maggio 2018, la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy;
- È necessario stabilire modalità organizzative, misure procedimentali e regole di dettaglio, che permettano a questo Ente di agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;

Visto il Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, approvato con deliberazione del Consiglio Comunale n. 12 del 20/06/2018, composto da numero 12 articoli, tra cui l'art. 9 riferito alla valutazione d'impatto sulla protezione dei dati;

Visto l'art 35 – I° comma - del Reg. UE 27-4-2016 n. 2016/679 che dispone:

> Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Il successivo terzo comma dispone:

> La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

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

Dato atto che il Comune di Miagliano con con deliberazione n. 13 del 16/11/2023 ha adottato il Regolamento per la videosorveglianza, e all'art. 7 è prevista specifica valutazione d'impatto sulla protezione dei dati personali in conformità a quanto sovra esposto;

Considerato quindi che è stata effettuata specifica valutazione d'impatto, di cui all'allegato A che forma parte integrante e sostanziale della presente deliberazione;

Ritenuto, pertanto, opportuno procedere all'approvazione del regolamento valutazione d'impatto sulla protezione dei dati;

Formula la seguente proposta di deliberazione

1. Di richiamare integralmente le premesse, di cui in narrativa argomentate, che costituiscono parte integrante del presente dispositivo;

2. Di approvare il Regolamento relativo alla valutazione d'impatto sulla protezione dei dati (DPIA) - impianto di videosorveglianza ex Reg. Comunale n. 13 del 16/11/2023, il quale viene allegato al presente atto per costituirne parte integrante e sostanziale (Allegato A);

3. Di trasmettere alla pubblicazione del presente provvedimento sul link "Amministrazione Trasparente" sul sito del Comune di Miagliano.

A questo punto

LA GIUNTA COMUNALE

- Udita la su estesa proposta di deliberazione e ritenutala meritevole di approvazione;
- VISTI i pareri favorevolmente espressi dal responsabile del servizio competente in ordine alla regolarità tecnica della proposta di deliberazione, ai sensi dell'art.49, 1° comma, del D.Lgs n. 267/2000;
- CON VOTI favorevoli ed unanimi espressi in forma palese

DELIBERA

DI APPROVARE integralmente la proposta di deliberazione di cui in premessa;

Successivamente

Di dichiarare all'unanimità la presente deliberazione immediatamente eseguibile ai sensi dell'art.134 comma 4 del D.Lgs n. 267/2000, in ordine alla necessità di provvedere a dare corso al deliberato, stante l'urgente necessità di prosieguo dell'iter amministrativo a fini di attuazione dei contenuti.

Letto, confermato e sottoscritto

Il Sindaco	Il Segretario Comunale
Firmato Digitalmente	Firmato Digitalmente
MOGNAZ Alessandro	DURIO Dr.ssa Carmen

COMUNE DI MIAGLIANO
Provincia di Biella

Valutazione d'impatto sulla protezione dei dati (DPIA)

Impianto di Videosorveglianza

Sommario

Premessa,

L'art 35 – I° comma - del Reg. UE 27-4-2016 n. 2016/679 dispone:

- Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Il successivo terzo comma dispone:

- La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

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

Sostanzialmente, le citate norme prevedono che allorchè un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggettiinteressati, di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il titolare, coadiuvato dal responsabile della protezione dei dati, se designato, è obbligato a svolgere una valutazione di impatto prima di dare inizio al trattamento (DPIA – Data protection impact assessment o anche PIA–Privacy impact assessment).

Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, esso esprime chiaramente la responsabilizzazione (accountability) del titolare nei confronti del trattamento da lui effettuato.

Il titolare infatti è tenuto, non soltanto, a garantire l´osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che
modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

Allo scopo di aiutare il titolare del trattamento in ordine alla necessità di realizzare la DPIA, il Gruppo di lavoro ex art. 29 ha individuato alcuni criteri per determinarne la necessità ovvero:

1. processo decisionale automatizzato;
2. monitoraggio sistematico;
3. dati sensibili o aventi carattere altamente personale;

4. trattamento dei dati su larga scala;
5. dati relativi a interessi vulnerabili;
6. uso innovativo o applicazione di nuove soluzioni tecnologiche;
7. ipotesi in cui il trattamento impedisce agli interessati di esercitare un diritto oavvalersi di un servizio.

Il Gruppo di lavoro ex art. 29 ha comunque suggerito di procedere alla valutazione d'impatto sulla protezione dei dati in caso di dubbio sulla necessità di realizzarla.

Alla luce di tutto ciò, Il Comune di Miagliano relativamente al trattamento dei dati derivanti dall'impianto di videosorveglianza ha predisposto la presente D.P.I.A, utilizzando il software open source "PIA" messo a disposizione dal CNIL (Autorità garante francese per la protezione dei dati personali), progetto a cui ha aderito successivamente l'Autorità garante italiana, inteso quale valido supporto ed indirizzo operativo.

Informazioni sulla PIA

Nome della P.I.A

Valutazione di impatto relativa all' impianto di Videosorveglianza del Comune di Miagliano

Nome autore

Comune di Miagliano

Data di creazione: anno 2023

Nome del DPO/RPD: i dati sono riportati sul sito internet istituzionale

Nome del responsabile del trattamento

Il responsabile del trattamento è individuato a norma del vigente regolamento sulla videosorveglianza comunale

Parere del DPO/RPD

In ottemperanza a quanto prescritto dall'art 35 del Reg UE 2016/678, il titolare del trattamento: Comune di Miagliano ha condotto la valutazione, sui potenziali rischi per i diritti e le libertà degli interessati, relativi al trattamento di videosorveglianza che il Comune effettua sul proprio territorio.

La valutazione è stata effettuata, preliminarmente attraverso una descrizione sistematica del trattamento e delle sue finalità, quali:

- 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 del territorio ed in particolare scoraggiare e prevenire l'increscioso e diffuso fenomeno dell'abbandono di rifiuti e la creazione di "micro- discariche", quando non risulta possibile, o si riveli inefficace, il ricorso a strumentie sistemi di controllo alternativi

ed in via incidentale:

- all'esigenza, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali a norma del D.Lgs. 51/2018

È stato valutato ed accertato la necessità del trattamento rispetto alle finalità sopra descritte e come vi sia la giusta proporzionalità dei dati trattati rispetto alle indicatefinalità.

Sono stati valutati tutti i rischi che possono derivare agli interessati dal trattamento ed in particolare per le quali possono derivare o comportare delle discriminazioni, usurpazione d'identità, pregiudizio alla reputazione, perdita di riservatezza.

Sono state valutate tutte le misure previste contro tali rischi, ovvero: la crittografia per i dati trattati, il controllo degli accessi logici, l'archiviazione dei dati , la sicurezza dei canali informatici, il controllo degli accessi fisici, la sicurezza dell'hardware, la gestione delle politiche di tutela della privacy, la gestione del personale, gli accessi diversificati, l'attività di manutenzione dell'impianto i Backup, la gestione delle postazioni, la tracciabilità, la vulnerabilità, la lotta contro il malware ed infine le misure antincendio ed ' è statoriconosciuto la loro valenza e la loro adeguatezza al contesto.

I rischi che potrebbero compromettere i diritti e le libertà degli interessati paiono quindi adeguatamente limitati

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Il trattamento è svolto nell'ambito dell'esecuzione di un compito di pubblico interesse o connesso all'esercizio di pubblici poteri.

Il parere degli interessati non è pertanto necessario in quanto è il legislatore che effettuaa priori un bilanciamento degli interessi coinvolti, assegnando maggiore rilevanza a taluno di essi senza però sacrificare del tutto i rimanenti.

Contesto

Panoramica del sistema

Quale è il trattamento in considerazione?

Il trattamento in considerazione è relativo al trattamento dei dati raccolti dall'impianto di videosorveglianza del Comune di Miagliano

In particolare, il Comune di Miagliano ai fini della:

- 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 del territorio ed in particolare scoraggiare e prevenirel'increscioso e diffuso fenomeno dell'abbandono di rifiuti e la creazione di "micro- discariche", quando non risulta possibile, o si riveli inefficace, il ricorso a strumentie sistemi di controllo alternativi.

ed in via incidentale:

- all'esigenza, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali a norma del D.Lgs. 51/2018

ha disposto, nel rispetto delle vigente normativa in materia e delle prescrizioni fornitedal Garante per la protezione dei dati personali, l'attivazione di un impianto di videosorveglianza urbana mediante l'installazione di telecamere/ fotocamere, debitamente segnalate.

Le apparecchiature sono indirizzate verso aree pubbliche o soggette a servitù di pubblico passaggio nonché su beni di proprietà comunale, individuati in ragione delle esigenze di sicurezza delle persone fisiche, tutela della sicurezza stradale, tutela del patrimonio comunale, tutela ambientale e sono collocate nelle vie, piazze o località comunali debitamente segnalate da cartellonistica di cui al vigente Regolamento comunale sulla videosorveglianza.

Il **titolare del trattamento:** è il Comune di Miagliano Piazza Martiri Libertà, 3 13816 Miagliano Tel. 015-2476035Fax: +39 0172/427016 email: miagliano@ptb.provincia.biella.it PEC: miagliano@pec.ptbiellese.it

Il responsabile della protezione dati: i dati di contatto sono disponibili sul sito internet istituzionale www.comune.miagliano.bi.it

Il responsabile del trattamento: BT ONE SOLUTION – VICINI A TE

Quali sono le responsabilità connesse al trattamento?

Le responsabilità connesse al trattamento sono, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, collegate ai rischi per i diritti e le libertà delle persone fisiche che vengono riprese dalle telecamere, per le quali possono derivare o comportare delle discriminazioni, usurpazione d'identità, pregiudizio alla reputazione, perdita di riservatezza

Ci sono standard applicabili al trattamento

Non ci sono standard applicabili al trattamento

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati sono le immagini delle persone fisiche nonché i dati identificativi delle auto (targhe) che vengono rilevate dalle telecamere o dalle fotocamere

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

Le immagini riprese dalle telecamere vengono trasmesse attraverso un collegamento hyperlan 5 GHZ ad una sala di controllo posta nei locali del comune, ove è posizionato una stazione di monitoraggio e controllo delle riprese effettuate dalle telecamere e dalla fotocamere.

Le telecamere, come sopra indicate consentono, tecnicamente, riprese video a colori incondizioni di sufficiente illuminazione naturale o artificiale, o, in caso contrario in bianco/nero.

Tali caratteristiche tecniche consentono un significativo grado di precisione e di dettagliodella ripresa.

In questa sede le immagini saranno visualizzate su di un monitor e registrate su di unsupporto magnetico.

Mentre le immagini fotografiche o video riprese dalle fototrappole sono trasferite su di unportale informatico in dotazione alla sala di controllo; il trasferimento di dati dalla fototrappola al portale informatico avviene manualmente senza collegamenti con altri sistemi o con altre reti pubbliche di telecomunicazioni, né attraverso l'accesso di altre periferiche ed è effettuato dal designato o dai preposti, muniti di di credenziali di accesso (nome utente e password)

L'accesso alla sala di controllo è consentito solamente alla persona designata al trattamento dei dati, ai preposti nonché al personale: addetto alla manutenzione degli impianti, designato dal responsabile del trattamento, per la pulizia dei locali e delle forzedell'ordine. Eventuali accessi di persone diverse da quelli innanzi indicate sono autorizzati periscritto, dal designato del trattamento.

Essi vigilano sul puntuale rispetto delle istruzioni e sulla corretta applicazione delle disposizione impartite dal titolare o dal designato del trattamento.

Il/I monitor degli impianti di videosorveglianza è collocato in modo tale da non permetterela visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

L’accesso alle immagini da parte del designato e di preposti si limita alle attività oggettodella sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione.

Nel caso in cui le immagini siano conservate, i relativi supporti sono custoditi, per l’interadurata della conservazione, in un armadio dotato di serratura, apribile solo dal designato.

L’accesso alle immagini ed ai dati personali è consentito:

- al designato
- ai preposti
- ai preposti alle indagini dell’Autorità Giudiziaria e di Polizia
- alla ditta che gestisce la manutenzione dell’impianto, nei soli casi in cui ènecessario l’accesso alle immagine per sua attività di manutenzione

Tutti gli accessi alla visione sono documentati mediante “log eventi del server di registrazione”.

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca deidati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

I dati trattati non saranno oggetto di diffusione a terzi, ad eccezione dei casi di espressae motivata disposizione dell’Autorità giudiziaria.

Designato al Trattamento è:

I tecnici della società VIDEOSORVEGLIANZA (responsabile del trattamento) accedono, in loco o da remoto, al sistema di videosorveglianza unicamente nella loro attività di manutenzione software ed hardware degli impianti.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono la:

- tutela della sicurezza urbana nei luoghi pubblici o aperti al pubblico, al fine di garantire il necessario grado di sicurezza dei cittadini e di tutte le persone che fanno parte della comunità;
- 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 del territorio ed in particolare scoraggiare e prevenirel’increscioso e diffuso fenomeno dell’abbandono di rifiuti e la creazione di “micro- discariche”, quando non risulta possibile, o si riveli inefficace, il ricorso a strumentie sistemi di controllo alternativi.

ed in via incidentale:

- all’esigenza, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali a norma del D.Lgs. 51/2018.

La videosorveglianza territoriale è quindi uno strumento funzionale allo svolgimento dei compiti istituzionali del Comune, cosi come indicato in questi anni da numerosi interventi legislativi, che hanno attribuito ai Sindaci ed ai Comuni specifiche competenze in materia di tutela dell'incolumità pubblica e della sicurezza urbana.

Al fine di tutelare la sicurezza e l'incolumità pubblica, non esistono, allo stato attuale, altri strumenti di vigilanza e controllo che garantiscano i risultati di un impianto di videosorveglianza, negli stessi termini di efficacia ed economicità, a fronte di un sacrificiodel tutto accettabile di una parte delle

libertà degli interessati.

In altri termini, si ritiene che sussista un **equo bilanciamento** tra l'interesse pubblico (nella specie, la tutela della sicurezza e dell'incolumità dei cittadini), ed i diritti degli interessati.

Quali sono le basi legali che rendono lecito il trattamento?

Le basi legali che rendono lecito il trattamento sono

- Art 6 –I° comma lettera e) del Regolamento EU 679/2016: “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”
- Art 6 del D.L. (cosiddetto “Decreto Sicurezza”) del 23 febbraio 2009 n. 11, recante misure urgenti in materia di sicurezza pubblica, convertito, con modificazioni,dall’art. 1 comma 1 della Legge del 23 aprile 2009, n. 38: “Per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza inluoghi pubblici o aperti al pubblico”.

Il trattamento dei dati personali è posto in essere nel pieno rispetto del Provvedimento dell'Autorità Garante per la protezione dei dati personali in materia di videosorveglianza (8 aprile 2010) ed in ultimo dalle linee guida dell’Europen Data Protection Board” - edpb - del 3/2019 sul trattamento dei dati personali .

Infine il Comune di Miagliano, con deliberazione C.C. n. 13/2023 ha approvato un Regolamento Comunale per l’utilizzo di sistemi di videosorveglianza.

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

Il dato personale raccolto (immagine) è limitato allo stretto necessario ed in modo assolutamente pertinente alla finalità per cui è trattato, assicurando il pieno rispetto del principio di minimizzazione dei dati.
L'attività di videosorveglianza è configurata, già in origine, limitando l'utilizzo di dati personali e di dati identificativi al minimo indispensabile, in modo da escluderne il trattamento quando non è strettamente necessario; in particolare quando le finalitàpossono essere perseguite mediante dati anonimi o limitando l’identificazione dei soggetti ai soli casi di necessità.

I dati sono esatti e aggiornati?

L'esattezza e genuinità del dato è garantita dalle misure tecniche che ne impediscono lamodifica.

Qual è il periodo di conservazione dei dati?

Le immagini registrate sono conservate per il tempo necessario per le finalità per lequali sono acquisite (art. 5, paragrafo 1, lett. c) ed e), del Regolamento).

In base al principio di responsabilizzazione (art. 5, paragrafo 2, del Regolamento), il titolare del trattamento ha individuato i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

In ottemperanza a quanto prescritto dall’art. 6, c. 8, del D.L. 23/02/2009, n. 11, per la tutela della sicurezza urbana e per la tutela ambientale, la conservazione dei dati, delle informazioni e delle immagini raccolte, è limitata ai sette giorni successivi alla rilevazione,fatte salve speciali esigenze di ulteriore conservazione" che possano derivare da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso.”

Per la tutela della sicurezza stradale la conservazione dei dati, delle informazioni e delleimmagini raccolte è limitata al tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;

Per la tutela dei beni patrimoniali del Comune la conservazione dei dati è limitata alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso incui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

I sistemi sono programmati in modo da operare la cancellazione automatica delle informazioni allo scadere del termine sopra previsto

Infine per i dati rilevati dalle foto trappole la loro conservazione rientra nei limiti previsti dall'art. 3.4 del "Provvedimento in materia di videosorveglianza 08/04/2010 del Garanteper la protezione dei dati personali e comunque non superiore alle 72 ore, in modo da garantire la conservazione degli stessi anche in relazione a festività e chiusure degli uffici.

Tale durata di conservazione potrà essere derogata per quelle immagini o video che danno luogo a contestazione di illeciti, per cui dovranno essere conservate per il periododi tempo strettamente necessario in riferimento: alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati che stanno per accedere o che si trovano in una zona video sorvegliata e dell'eventuale registrazione, mediante un modello semplificativo di informativa "minima", cosi come previsto dalle linee guide del Garante dell'8 aprile 2010 edalle linee guida dell'"Europen Data Protection Board" - edpb - del 3/2019 sul trattamento dei dati personali attraverso dispositivi videosorveglianza

Tale informativa è collocata prima del raggio di azione della telecamera, nelle sueimmediate vicinanze.

Ha un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza èeventualmente attivo in orario notturno.

Inoltre sul sito istituzionale del Comune, accessibile tramite un collegamento diretto dalla homepage, è pubblicata l'informativa, contenente 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 dall'art. 13 del Regolamento Europeo, relativo alla protezione delle persone fisiche con riguardo al trattamento dei datipersonali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamentoe perseguimento di reati o esecuzione di sanzioni penali.

In tale informativa è riportata l'indicazione della esatta collocazione di tutti gli impianti di videosorveglianza comunale con indicazione della natura e finalità di essi.

Detta informativa sarà integrata in relazione all'incremento dimensionale dell'impianto e all'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo.

Relativamente alla videosorveglianza per il controllo della sicurezza stradale l'informativaè quella prevista dalla normativa di settore.

Ove applicabile: come si ottiene il consenso degli interessati?
La base giuridica del trattamento è lo svolgimento di un compito connesso all'esercizio diun pubblico interesse o di pubblici poteri.

Non è pertanto richiesto il consenso dell'interessato.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità deidati?
In relazione al trattamento dei propri dati personali l'interessato, dietro presentazione diapposita istanza, ha diritto:

a) di ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;

b) Di essere informato sugli estremi identificativi del titolare, del responsabile del trattamento, del responsabile della protezione dei dati, oltre che, sulle finalità e lemodalità del trattamento dei dati;

c) di ottenere, a cura del designato del trattamento, senza ritardo e comunque nonoltre 15 giorni dalla data di ricezione della richiesta, ovvero di 30 giorni previa comunicazione, se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo:

   1. la conferma dell'esistenza o meno di dati personali che lo riguardano, nonché la trasmissione in forma intelligibile dei medesimi dati e della loro origine, procedendo, ove tecnicamente possibile, alla cancellazione dei dati di altre persone presenti nell'immagine richiesta; una nuova richiesta non può essereinoltrata da uno stesso soggetto se non trascorsi almeno novanta giorni da una precedente istanza, fatta salva l'esistenza di giustificati motivi;

   2. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattatiin 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;

   3. di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Per ciascuna delle richieste di cui alla lettera c), n. 1), può essere chiesto all'interessato, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, secondo le modalità previste dalla normativa vigente.

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

Nell'esercizio di tali diritti l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistereda persona di fiducia.

L'istanza può essere trasmessa al titolare o al designato anche mediante lettera raccomandata, telefax o posta elettronica o comunicata oralmente, che dovrà provvederein merito entro e non oltre quindici giorni.

Nel caso di esito negativo alla istanza 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.

Il diritto di portabilità dei dati non è esercitabile stante l'inapplicabilità dell'art. 20 Reg. 2016/679/UE al trattamento oggetto di valutazione.

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

Non è in concreto esercitabile, in riferimento alle immagini registrate, il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca deidati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

Il diritto di cancellazione può essere avanzato dagli interessati inoltrando appositarichiesta al Titolare del trattamento, al Designato al trattamento o al Responsabile per la protezione dei dati personali (Data Protection Officer, DPO), secondo la procedura di cuial precedente punto, qualora ricorrano le condizioni di cui all'art. 17 Reg. 2016/679/UE.

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

Gli interessati possono esercitare i loro diritti di limitazione e di opposizione al trattamento contattando il Titolare del trattamento, il Designato al trattamento o il Responsabile perla protezione dei dati personali (Data Protection Office, DPO), secondo quanto indicato alprecedente punto

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

Gli obblighi del Responsabile del trattamento sono assunti mediante specifica determina di affidamento di incarico e successiva stipula di contratto, con nomina di responsabile del trattamento, ai sensi dell'art 28 del Reg U.E 2016/679.

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

I dati trattati non vengono trasferiti al di fuori dell'Unione europea.

Rischi

Misure esistenti o pianificate

Crittografia

Le comunicazioni radio sono crittografate con il protocollo di sicurezza **WPA2/PSK.**

Controllo degli accessi logici

Solo il Designato o i preposti possono accedere alle immagini in diretta ed alle immagini conservate sul server attraverso dei propri username e delle proprie password.
Il sistema segnala all'utente l'utilizzo di una password considerata troppo debole, invitandolo così ad utilizzarne una adeguata.

Tracciabilità

Ogni operazione compiuta sui sistemi è registrata nel log degli eventi.
Il log eventi ha una durata programmabile e conserva tutti gli eventi di sistema (come, adesempio, gli accessi da parte degli utenti).
Ad oggi il sistema è programmato per salvare gli eventi degli ultimi 180 giorni.

Archiviazione

L'archiviazione sugli hard disk è fissata secondo i termini di conservazione dei dati come sopra indicato specificamente.
Il tempo di mantenimento delle immagini e registrazioni è di 10 (DIECI) giorni.
Successivamente, i dati più vecchi sono sovrascritti automaticamente.

Minimizzazione dei dati

Sono raccolte le sole immagini di contesto, senza estrapolazione automatica dei di dati biometrici o di altre categorie particolari di dati.

Sono letti in automatico i dati relativi alle targhe dei veicoli che transitano sotto alcune telecamere più evolute (il cui elenco è rintracciabile nelle premesse del presente documento nonché nell'informativa pubblicata sul sito internet del Comune).

Vulnerabilità

I software e l'hardware sono aggiornati al bisogno durante l'attività di manutenzionecompiuta dal Responsabile del trattamento dei dati.

Lotta contro il malware

Il server, di tipo Linux, e Window 10 per la letture delle targhe non è collegato direttamente alla rete internet.

Gestione postazioni

Il PC, sito nell'ufficio della sala di controllo che necessita di apposita chiave per l'accesso, è utilizzabile solo dal designato o dai preposti muniti di credenziali di accesso personali.
Il server al momento non è munito di monitor e non necessita di accesso da parte delpersonale in loco.
Un regolamento comunale disciplina le procedure di accesso alle postazioni.

Backup

Il sistema di salvataggio è composto da n. 4 (QUATTRO) dischi in RAID 5.
Viene eseguito un Backup o una ridondanza dei dati con metodo RAID 5 che rende il sistema resiliente alla perdita di uno o più dischi e poterli rimpiazzare senza interrompereil servizio.

Manutenzione

Il Responsabile del trattamento provvede, secondo quanto stabilito da contratto, alla manutenzione programmata.
L'attività è condotta in outsourcing.

Sicurezza dei canali informatici

Misure di sicurezza WPA2 e password.
Il server che ospita le immagini può essere raggiunto dalle rete internet solamente dall'IPpubblico della connessione del responsabile del trattamento, ditta "S.T. S.r.l.", il server infine, è collegato ad un router con opportune regole di Firewall, riducendo così drasticamente i rischi di attacco da parte di cyber criminali.

Controllo degli accessi fisici

Il computer da cui si accede al server è collocato in un apposito locale chiuso a chiave, accessibile solo al designato al trattamento, ai preposti, a tecnici della manutenzione designati dal responsabile del trattamento e al personale della pulizia, tutti ritualmentenominati.

Sicurezza dell'hardware

La rete, a servizio della videosorveglianza è isolata e non è connessa ad internet; oltre alle credenziali personali è presente una password sul PC di accesso al server.

Mentre il P.C. server per la lettura delle targhe è connessa alla rete per l'attività di manutenzione dell'impianto e per i collegamenti ai servizi esterni, quali, per la letturadelle targhe il collegamento all'ufficio della motorizzazione provinciale.

Politica di tutela della privacy

Si è proceduto alla nomina del Data Protection Officer.
Il designato al trattamento vigila inoltre sulla genuinità del trattamento dei dati.

Gestione delle politiche di tutela della privacy

Il Titolare del trattamento ha approvato un Regolamento comunale relativo alla protezione dei dati personali oltre ad uno specifico regolamento in materia di videosorveglianza.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L'ente si adopera nel rispetto della normativa vigente del Garante della Privacy per la gestione di potenziali incidenti di sicurezza e violazione dei dati personali.

Gestione del personale

Il personale autorizzato al trattamento ha ricevuto una specifica formazione in merito alla protezione dei dati personali, cosi come prevista dal vigente regolamento europeo 2016/678 e del successivo regolamento comunale di attuazione del regolamento europeo nonché del regolamento di disciplina del servizio di videosorveglianza.

La nomina del designato dà conto del dovere di riservatezza cui sono tenuti, in base allanormativa vigente.

Accessi diversificati

La password è diversificata tra il Designato al trattamento, i preposti al trattamento ed il Responsabile del trattamento (che è il manutentore del sistema) in modo da poter identificare chi accede al sistema.

Misure antincendio

Il trattamento dei dati avviene nel pieno rispetto degli obblighi normativi in materia di prevenzione incendi.

Nella sede municipale sono presenti n. adeguati estintori come da normativa, di cui n. 1 posto nelle immediate vicinanze dell'ufficio preposto.

Accesso illegittimo ai dati

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

Perdita o alterazione, anche irreversibile dei dati. Perdita o alterazione, anche irreversibile dei programmi.Impossibilita temporanea di accesso di dati.
Impossibilita temporanea di accesso si programmi.
Per gli interessati: lesione del diritto d'immagine, lesione del diritto alla riservatezza, percezione di insicurezza

Quali sono le principali minacce che potrebbero concretizzare il rischio?
Attacco da remoto ai sistemi da parte di hacker, accesso non autorizzati alla sala di controllo, visione dei monitor in diretta per una finalità illegittima se non illecita

Quali sono le fonti di rischio?
Fonti umane interne - Personale non adeguatamente preparato - Fonti umane esterne - Hacker

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Crittografia, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Gestione postazioni, Lotta contro il malware, Politica di tutela della privacy, Vulnerabilità, Gestione del personale, Accessi diversificati, Gestione delle politiche di tutela della privacy, Controllo degli accessi fisici, Sicurezza dei canali informatici, Manutenzione

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

La gravità delle conseguenze di un ipotetico accesso non autorizzato agli impianti di videosorveglianza sono del tutto trascurabili.

Chi accede agli impianti può visionare unicamente immagini riguardanti persone e cose presenti in un pubblico spazio (territorio urbano) o, in alcuni casi, il transito di un determinato veicolo, in precise circostanze di tempo e di luogo.

Non essendoci impianti con caratteristiche di riconoscimento biometrico, è impossibile associare univocamente una figura umana che compare nelle immagini ad una persona fisica (a meno che l'intruso non conosca personalmente l'interessato).

E' invece possibile, in via ipotetica, riscontrare passaggi di veicoli attraverso una ricercamirata per targa.

Qualora un interessato venisse a conoscenza dell'intrusione, scaturirebbero conseguenze psicologiche di bassissimo impatto quali, a titolo esemplificativo, semplice fastidio e percezione di pericolo non particolarmente intensa con riferimento all'impressione di violazione della propria riservatezza, senza pur patire un danno reale.

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

Le misure di sicurezza paiono adeguate a proteggere i dati personali trattati da accessinon autorizzati in considerazione del contesto degli impianti che saranno in funzione.
La probabilità di concretizzazione del rischio di accesso illegittimo ai dati è trascurabile,soprattutto per quanto concerne gli attacchi di soggetti esterni all'ente.

Trascurabile inoltre la probabilità di accesso illegittimo ai dati ad opera di fonti umaneinterne.

Gli autorizzati al trattamento sono soggetti specifici (e numericamente limitati) in possesso di credenziali personali (e ciò è valido anche in relazione al Responsabile del trattamento).

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Lesione al diritto all'immagine, Lesione all'integrità del dato personale, Impossibilità di tutela a seguito di un reato subito, Percezione di insicurezza

Quali sono le principali minacce che potrebbero consentire la concretizzazione delrischio?
Attacco da remoto ai sistemi da parte di hacker , Accesso non autorizzati alla sala dicontrollo , Visione dei monitor in diretta per una finalità illegittima se non illecita

Quali sono le fonti di rischio?
Fonti umane interne, - Personale no adeguatamente preparato Fonti umane esterne -Hacker

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? Crittografia, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Manutenzione, Sicurezza deicanali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tuteladella privacy, Gestione delle politiche di tutela della privacy, Accessi diversificati, Gestione del personale

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali edelle misure pianificate?
Limitata, Una modificazione indesiderata delle immagini comporterebbe un rischiolimitato con riguardo al profilo psicologico dell'interessato.

Il senso di violazione della propria riservatezza sarebbe apprezzabile, sebbene priva didanni irreparabili.

Ciò potrebbe comportare un disturbo di contenuta gravità ma oggettivo, soprattutto nellepersone più suscettibili.

Le immagini alterate potrebbero essere utilizzate, in linea teorica, per scherni, intimidazioni o ricatti verso gli interessati ad opera di malintenzionati.

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

Trascurabile, Sebbene il rischio zero sia da considerarsi un'utopia a carattere precipuamente teorico, la modifica dell'immagine raccolta da una telecamera di videosorveglianza è un'operazione tecnicamente molto complessa.

Il rapporto costi/benefici tra i mezzi impiegati ed i risultati ottenuti per compiere l'azioneillecita risulta davvero sproporzionato.

In ogni caso, le misure di sicurezza che sono state adottate contribuiscono ad abbattere drasticamente la già scarsissima probabilità di verificazione dell'evento.

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Lesione alla integrità del dato personale, Impossibilità di tutela a seguito di un reatosubito, Percezione di insicurezza

Quali sono le principali minacce che potrebbero consentire la materializzazione delrischio?
Attacco da remoto, Accesso non autorizzati alla sala di controllo, Malfunzionamenti fisicidei sistemi, Eventi naturalistici

Quali sono le fonti di rischio?
Fonti umane interne, - Personale no adeguatamente preparato Fonti umane esterne -Hacker

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio? Crittografia, Controllo degli accessi logici, Archiviazione, Sicurezza dei canali informatici,Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione delle politiche di tutela della privacy, Gestione del personale, Accessi diversificati, Politica di tutela della privacy,Manutenzione, Backup, Gestione postazioni, Tracciabilità, Vulnerabilità, Lotta contro il malware, Misure antincendio

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, Una perdita indesiderata delle immagini comporterebbe un rischio limitato conriguardo al profilo psicologico dell'interessato.

Il senso di violazione della propria riservatezza sarebbe apprezzabile, sebbene priva didanni irreparabili.

Ciò potrebbe comportare un disturbo di contenuta gravità ma oggettivo, soprattutto nellepersone più suscettibili.

La perdita del dato comporterebbe l'impossibilità di utilizzare le immagini per reprimere ireati commessi, con conseguente danno materiale e morale per l'interessato che accresce in relazione alla gravità del reato subito.

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

Le misure di sicurezza che sono state adottate contribuiscono ad abbattere drasticamente la probabilità di verificazione di una perdita dei dati.

Le misure antincendio, sebbene non soggette ad automatismi, sono proporzionate allemodeste dimensioni del server ospitato.

La politica di memorizzazione consente di salvare le immagini su più dischi fisici, indipendenti tra loro, e garantire una continuità operativa (grazie alla tecnologia RAID) anche nel caso venisse meno uno dei supporti e prima che esso sia sostituito.
Le misure informatiche e fisiche paiono adeguate a prevenire la perdita dei dati trattati.

La politica di manutenzione periodica contribuisce a prevenire la probabilità di verificazione della perdita indesiderata di dati a causa di malfunzionamento degli apparatitecnici.

Il rischio di terremoti, che potrebbero ipoteticamente danneggiare i supporti, è di per sé trascurabile. Secondo la classificazione del rischio sismico condotta dal Dipartimento della Protezione Civile, il comune di Miagliano è sito in zona 4

La presente valutazione d’impatto verrà aggiornata ogni qualvolta verrà integrato o modificato l’impianto, sia con l’innesto di nuove telecamere, sia con una nuova o diversatecnologia

Il Titolare del trattamento
Comune di Miagliano

Il Data Protection Officer
Progetto Informatica