COMUNE DI CASTEL RITALDI

Provincia di Perugia

DPIA – VIDEOSORVEGLIANZA COMUNALE

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) AI SENSI DEL REGOLAMENTO (UE) N.679/2016

Informazioni sulla DPIA

Nome della DPIA: Valutazione sul sistema di Videosorveglianza Comunale

Nome autore: Segretario Comunale
Data di creazione: 22/01/2024

Nome del DPO/RPD: Avv. Luca Iadecola

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Non si ritiene opportuno procedere alla richiesta di alcun parere agli interessati per impossibilità oggettiva.

Panoramica del trattamento
Le operazioni di trattamento dati che il Comune di Castel Ritaldi 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 Castel Ritaldi 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 reci- proco rispetto e di rispetto delle Istituzioni e delle loro funzioni.
I sistemi di videosorveglianza utilizzati dal Comune di Castel Ritaldi sono, infatti, proporzionati ed efficaci rispetto alle finalità prefissate e sono tali da non comportare rischi ultronei rispetto a quelli inseriti in un contesto di normale funzionalità dei sistemi tecnologici delle tipologie in uso, avuto anche riguardo alla utilizzazione dei medesimi strumenti anche in altri contesti urbani, considerazione questa che consente di accrescere la fiducia e la credibilità degli strumenti stessi.
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, anche con dispositivi idonei alla lettura targhe;

2) sistema di videosorveglianza ambientale con "videotrappole" amovibili posizionate in prossimità dei luoghi destinati al gettito di rifiuti ovvero in aree presso le quali è stato rilevato ovvero potrebbe verificarsi il gettito irregolare e abusivo di rifiuti.

Il trattamento operato dagli agenti di Polizia Locale, interamente o parzialmente automatizzato, dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e fototrappolaggio attivati nel territorio dell'Ente, ai sensi del Reg. UE 2016/679, della Direttiva UE 2016/680, in osservanza delle disposizioni contenuti nel "decalogo" del 8 aprile 2010 dal Garante della Privacy e del Codice Nazionale sulla Privacy D.lgs. n. 196/2003.

L'impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati e ha come obbiettivo di verificare e garantire la protezione dei dati personali di tutti coloro che entrano in contatto o in relazione con l'attività di videosorveglianza e fototrappolaggio.

La raccolta ed ogni altra attività di trattamento dei dati degli interessati acquisiti dal Titolare, mediante sistemi di videosorveglianza, vengono effettuate da quest'ultimo presso la centrale operativa ubicata presso il Servizio di Polizia Locale, sotto la responsabilità del Designato al trattamento dei dati, nel rispetto delle misure di sicurezza e prescrizioni imposte dal Regolamento Europeo 679/2016 e del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, o da soggetti da esso delegati (appositamente selezionati e dotati della necessaria professionalità), con procedure informatizzate.

I dati raccolti mediante il sistema di videosorveglianza, oggetto del trattamento, sono trattati ed utilizzati per finalità istituzionali conformi a quelle demandate all'ente dal D.Lgs. 18 agosto 2000, n. 267, dall'art. 6 del DL 23 febbraio 2009, n. 11, convertito nella legge 23 aprile 2009, n. 38, nonché dallo Statuto Comunale e dai Regolamenti Comunali vigenti, ed in particolare per la:

- 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;
- 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, decoro urbano e polizia amministrativa.

Oltre che per le finalità sopraindicate, i dati raccolti mediante il sistema di videosorveglianza saranno trattati ed utilizzati al fine di contrastare l'attività di conferimento abusivo di rifiuti.

Soggetti coinvolti e le responsabilità connesse al trattamento

I soggetti coinvolti nell'attività di trattamento sono:

a) il titolare del Trattamento, ovvero il Comune di Castel Ritaldi nella persona del Sindaco pro tempore;
b) il Designato al trattamento dei dati rilevati con apparecchi di videosorveglianza, ovvero il Responsabile del Servizio di Polizia Locale, il quale può delegare in forma scritta le proprie funzioni;
c) tutti gli operatori della Polizia Locale designati al trattamento dei dati;
d) la società esterna che ha accesso ai dati (TargaSystem s.r.l.), giusto atto di nomina prot. n. 8260/2023 a responsabile del trattamento ai sensi dell'art. 28 GDPR.

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.

Standard applicabili al trattamento

Attualmente gli standard per sistemi di videosorveglianza urbana non esistono ma possiamo appoggiarci alla combinazione di più norme di settore.

Non vi sono standard direttamente applicabili al trattamento.

REGOLAMENTO PER LA DISCIPLINA DEL SISTEMA DI VIDEOSORVEGLIANZA COMUNALE (approvato con delibera di C.C. n. 44 del 28/12/2023).

Dati, processi e risorse di supporto

I dati trattati consistono in immagini e video registrati sul piano operativo; la registrazione è attiva 24 ore su 24 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.

Gli impianti di videosorveglianza sono installati sul territorio comunale e possono essere sia fissi che mobili. Registrano immagini che possono permettere di identificare in modo diretto o indiretto le persone riprese e fanno riferimento a informazioni riconducibili a dati personali (caratteristiche fisiche abitudini, stili di vita, posizione geografica).

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 videosorveglianza installati sul territorio cittadino.

La disponibilità tempestiva di immagini presso la Sala Operativa della 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 videosorveglianza in dotazione alla Polizia Locale, compresi i sistemi di lettura targhe, 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 videosorveglianza 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 videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità sopra citate, 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.

Le immagini videoregistrate sono conservate per un periodo di 7 giorni, fatte salve esigenze ulteriori di conservazione nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria o della Polizia Giudiziaria o all'eventuale esercizio del diritto di accesso riconosciuto all'interessato ai sensi dell'art. 15 GDPR. Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione - ove tecnicamente possibile - mediante sovra-registrazione, con modalità tali da rendere non più utilizzabili i dati cancellati.

Risorse di supporto ai dati

Sistema di videosorveglianza urbana

Sistema di lettura targhe:

N. 3 KIT varco doppia corsia con larghezza a 6m circa, telecamera ANPR, OCR lettura targhe, rilevamento fino a 2 corsie, risoluzione 3Mpx, velocità di rilevamento fino a 250 km/la, certificazione UNI 10772/2016, Tecnologia DUAL SHUTTER con immagini a colori anche di notte, doppio fotogramma (dettaglio + contesto) riconoscimento Marca, Modello e Colore, classificazione veicoli (9 classi).

Licenza software connessione video, licenza software collegamento ministeriale.

Video/Fototrappole:

n.1 IP camera Varifocal opt fissa 3.6mm 4mpx monosensore
n.1 IP camera 5mpx multisensore (4) panoramica 360°
n.1 IP camera 5mpx multisensore (4) panoramica 360°
n.3 CpE Radio PtP 5hz con deflettorte max 40cm
Server NVR per registrazioni
n. 1 Radio Faro 5.8ghz freq. libera composto: elettronica Motorola + Antenna RF Elements R120

I dati personali sono raccolti attraverso riprese video effettuate da sistemi di telecamere a circuito chiuso installate in corrispondenza delle principali strade, piazze, giardini comunali ed aree pertinenziali agli edifici scolastici, luoghi pubblici ed immobili di proprietà comunale, ed eventualmente, di privata proprietà in caso di convenzione con l'ente Comune, ubicati nel territorio comunale.
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, che potrà, esclusivamente per il perseguimento dei fini istituzionali, eventualmente digitalizzare o indicizzare le immagini. Possono altresì adottare il sistema OCR di lettura targa.
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

Scopi del trattamento
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 Castel Ritaldi, attraverso il Servizio di Polizia Locale, effettua il trattamento di dati personali mediante impianti di videosorveglianza urbana, sia di osservazione che di contesto.
In particolare, l'uso di tutti i sistemi e tipologie di videosorveglianza 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 videosorveglianza dd. 08/04/2010;
b) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale ed a prevenire eventuali atti di vandalismo o danneggiamento;
c) 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;
d) al monitoraggio del traffico veicolare, al fine di prevenire o gestire problematiche inerenti alla viabilità;
e) 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 videosorveglianza dd. 08/04/2010;
f) rilevare violazioni al Codice della strada, contestati nella immediatezza, mediante l'uso di sistemi OCR (Optical Character Recognition) per riconoscimento delle targhe veicolari;
g) tutelare l'ordine e la sicurezza pubblica e prevenire, accertare e reprimere i reati mediante il controllo dei veicoli in transito; le informazioni delle targhe inserite in "liste di controllo" particolari potranno essere condivise con le altre Forze dell'Ordine a seguito di specifico "Protocollo operativo" predisposto e sottoscritto dal Comitato provinciale per l'ordine e la sicurezza pubblica;
h) supportare operazioni di protezione civile.

Basi legali che rendono lecito il trattamento
Sulla base di quanto sopra indicato 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.

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

I dati vengono raccolti solo per l'attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale e per la ricostruzione della dinamica di eventuali atti vandalici o fatti criminosi o azioni di teppismo nei luoghi pubblici di principale frequentazione, anche a tutela del patrimonio pubblico.
I dati raccolti ed elaborati vengono minimizzati utilizzando le informazioni strettamente necessarie all'erogazione del servizio

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 videosorveglianza, 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.
Le immagini videoregistrate sono conservate per un periodo di 7 giorni nella centrale di registrazione, fatte salve esigenze ulteriori di conservazione nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria o della Polizia Giudiziaria o all'eventuale esercizio del diritto di accesso riconosciuto all'interessato ai sensi dell'art. 15 gdpr.
Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione, ove tecnicamente possibile mediante sovra-registrazione, con modalità tali da rendere non più utilizzabili i dati cancellati.

Informativa al trattamento degli 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", così come previsto dalle linee guide del Garante dell'8 aprile 2010 e dalle linee guida dell'European 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 sue immediate vicinanze.
Ha un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza è eventualmente attivo in orario notturno.
Si specifica inoltre che nella sezione "privacy" del sito web istituzionale del Comune di Castel Ritaldi viene riportata l'informativa completa sul trattamento dei dati di videosorveglianza ai sensi dell'art. 13 del GDPR UE 679/2016.

Il consenso degli interessati
La base giuridica del trattamento è lo svolgimento di un compito connesso all'esercizio di un pubblico interesse o di pubblici poteri.
Pertanto non è richiesto il consenso dell'interessato.

Esercizio degli interessati a esercitare i diritti di accesso e di portabilità dei dati
Agli interessati sono riconosciuti, ove concretamente applicabili, i diritti di cui agli artt. 15 – 22 gdpr.
In relazione al trattamento dei propri dati personali l'interessato, dietro presentazione di apposita 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 le modalità del trattamento dei dati;
c) di ottenere, a cura del personale preposto al trattamento, senza ritardo e comunque non oltre 15 giorni dalla data di ricezione della richiesta, oppure 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

essere inoltrata 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 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;
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), 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 essere esercitati 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 assistere da persona di fiducia.
L' istanza può essere trasmessa al titolare o al designato anche mediante lettera raccomandata, telefax o posta elettronica.
Il diritto di portabilità dei dati non è esercitabile stante l'inapplicabilità dell'art. 20 Reg. 2016/679/UE al trattamento oggetto di valutazione.
Le istanze relative all'esercizio dei diritti dell'interessato possono essere indirizzate al Titolare del trattamento al seguente indirizzo: privacy@comune.castel-ritaldi.pg.it oppure via posta, presso la sede del Comune.
L'interessato, qualora non sia soddisfatto del riscontro fornito alle sue richieste dal Titolare del trattamento o dal Responsabile protezione dei dati, può proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali, sede in Roma, Piazza Venezia n. 11, www.garanteprivacy.it .
Il cittadino di altro Stato membro dell'Europea ha facoltà di rivolgersi all'autorità di controllo del proprio paese.

Esercizio degli interessati ai 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 dei dati 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 apposita richiesta al Titolare del trattamento, al preposto al trattamento o al Responsabile per la protezione dei dati personali (Data Protection Officer, DPO), secondo la procedura di cui al precedente punto, qualora ricorrano le condizioni di cui all'art. 17 Reg. 2016/679/UE.

Esercizio degli interessati ai 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 Preposto al trattamento o il Responsabile per la protezione dei dati personali (Data Protection Office, DPO), secondo quanto indicato al precedente punto.

Obblighi dei responsabili del trattamento
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.

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

Anonimizzazione
Qualora dalle immagini riprese si evincano dati personali appartenenti a terzi, il personale autorizzato provvede ad anonimizzarli prima di renderli noti

Crittografia
Le comunicazioni radio sono crittografate.

Controllo degli accessi logici
Solo il personale autorizzato 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, ad esempio, 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 7 (SETTE) 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.

Vulnerabilità
I software e l'hardware sono aggiornati al bisogno durante l'attività di manutenzione compiuta dal Responsabile del trattamento dei dati.
I pc in uso sono dotati di sistemi operativi e antivirus costantemente aggiornati.
L'accesso ai dati è consentito unicamente agli autorizzati, muniti di account personale

Lotta contro il malware
L'antimalware è regolarmente installato e costantemente aggiornato.

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 non necessita di accesso da parte del personale in loco. Il regolamento comunale disciplina le procedure di accesso alle postazioni.

Backup
I backup vengono effettuali quotidianamente.

Manutenzione
Il Responsabile del trattamento provvede, secondo quanto stabilito da contratto, alla manutenzione programmata. L'attività è condotta in outsourcing.
TargaSystem srl, Circonvallazione Clodia, 163-167, 00195 Roma (RM).
Atto di nomina a responsabile esterno del trattamento art. 28 gdpr, prot. n. 8260 del 20/12/2023.

Sicurezza dei canali informatici
Misure di sicurezza WPA2 e password.
Firewall: ZyXEL ZyWALL USG 100.

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 ritualmente nominati.

Sicurezza dell'hardware
Oltre alle credenziali personali è presente una password sul PC di accesso.
Mentre il Pc 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 lettura delle targhe il collegamento all'ufficio della motorizzazione.

Gestione delle politiche di tutela della privacy
Si è proceduto alla individuazione del Data Protection Officer.
Il designato al trattamento vigila inoltre sulla genuinità del trattamento dei dati.
Il Titolare del trattamento ha approvato uno specifico regolamento in materia di videosorveglianza.
Si è proceduto ad uno corso di formazione per il personale dipendente.

Gestione del personale
Il personale autorizzato al trattamento riceve annualmente dal DPO una formazione generale in merito alla protezione dei dati personali, cosi come prevista dal vigente regolamento europeo 2016/678 e del regolamento di disciplina del servizio di videosorveglianza comunale, nonché sessioni di formazione su specifici argomenti, all'occorrenza.
La nomina del designato dà conto del dovere di riservatezza cui sono tenuti, in base alla normativa 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.

Principali impatti sugli interessati se il rischio si dovesse concretizzare
Perdita o alterazione, anche irreversibile dei dati.
Perdita o alterazione, anche irreversibile dei programmi.
Impossibilità temporanea di accesso di dati.
Impossibilità temporanea di accesso si programmi.
Per gli interessati: lesione del diritto d'immagine, lesione del diritto alla riservatezza, percezione di insicurezza.
Lesione al diritto all'immagine; Lesione all'integrità del dato personale; Impossibilità di tutela a seguito di un reato subito; Percezione di insicurezza.

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.

Minacce che potrebbero consentire la materializzazione del rischio
Attacco da remoto; Accesso non autorizzati alla sala di controllo; Malfunzionamenti fisici dei sistemi; Eventi naturalistici

Fonti di rischio
Fonti umane interne; Personale non adeguatamente preparato; Fonti umane esterne; Hacker.

Misure che contribuiscono a mitigare il rischio
Minimizzazione dei dati, Gestione postazioni, Lotta contro il malware, Gestione del personale, Accessi diversificati, Gestione delle politiche di tutela della privacy, Sicurezza dei canali informatici, Manutenzione, Anonimizzazione, Crittografia, Controllo degli accessi logici, Archiviazione, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione del personale, Accessi diversificati, Politica di tutela della privacy, Manutenzione, Backup, Tracciabilità, Vulnerabilità, Lotta contro il malware, Misure antincendio.

Gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate
Accettabile: la gravità delle conseguenze di un ipotetico accesso non autorizzato agli impianti di videosorveglianza sono accettabili. 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 non si conosca personalmente l'interessato). È invece possibile, in via ipotetica, riscontrare passaggi di veicoli attraverso una ricerca mirata per targa.
Limitata: una modificazione indesiderata delle immagini comporterebbe un rischio limitato con riguardo al profilo psicologico dell'interessato. Il senso di violazione della propria riservatezza sarebbe apprezzabile, sebbene priva di danni irreparabili. Ciò potrebbe comportare un disturbo di contenuta gravità ma oggettivo, soprattutto nelle persone più suscettibili. Le immagini alterate potrebbero essere utilizzate, in linea teorica, per scherni, intimidazioni o ricatti verso gli interessati ad opera di malintenzionati.
Limitata: una perdita indesiderata delle immagini comporterebbe un rischio limitato con riguardo al profilo psicologico dell'interessato. Il senso di violazione della propria riservatezza sarebbe apprezzabile, sebbene priva di danni irreparabili. Ciò potrebbe comportare un disturbo di contenuta gravità ma oggettivo, soprattutto nelle persone più suscettibili. La perdita del dato comporterebbe l'impossibilità di utilizzare le immagini per reprimere i reati commessi, con conseguente danno materiale e morale per l'interessato che accresce in relazione alla gravità del reato subito.

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'azione illecita 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.
Le misure di sicurezza paiono adeguate a proteggere i dati personali trattati da accessi non 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.

Allegato: Regolamento per la disciplina della videosorveglianza nel territorio comunale

Il Titolare del trattamento
Il Sindaco
Elisa Sabbatini

Il Data Protection Officer
Avv. Luca Iadecola