COMUE DI CHERASCO

Provincia di Cuneo

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 soggetti interessati, 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 o avvalersi 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 Cherasco 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 Cherasco

Nome autore

Comune di Cherasco

Data di creazione

11.11.2021

Nome del DPO/RPD

dott. Mazzarella Luigi

Nome del responsabile del trattamento

Il responsabile del trattamento è S.T. S.r.l." di Udine, con sede in Viale Tricesimo, n.184/3; Tel. 800939310., email: info@gruppost.it - aministrazione@gruppost.it

Parere del DPO/RPD

In ottemperanza a quanto prescritto dall'art 35 del Reg UE 2016/678, il titolare del trattamento : Comune di Cherasco ha condotta 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 strumenti e 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

E 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 indicate finalità.

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 stato riconosciuto 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 effettua a 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 Cherasco

In particolare, il Comune di Cherasco 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 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 strumenti e 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 fornite dal 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 seguenti vie, piazze o località:

- Via Vittorio Emanuele II – Torre Municipale CAM1 per finalità di tutela della sicurezza urbana;
- Via Vittorio Emanuele II – Torre Municipale CAM2 per finalità di tutela della sicurezza urbana;
- Via Vittorio Emanuele II – Torre Municipale CAM3 per finalità di tutela della sicurezza urbana;
- Via Vittorio Emanuele II – Torre Municipale CAM4 per finalità di tutela della sicurezza urbana;
- Piazza Mockmùhl per finalità di tutela della sicurezza urbana;
- Via Garibaldi intersezione via Vittori Emanuele per finalità di tutela della sicurezza urbana;
- Piazza degli Alpini – Giardini pubblici per finalità di tutela della sicurezza urbana;
- Via Sant'Iffredo – Centro Anziani CAM1 per finalità di tutela della sicurezza urbana e tutela del patrimonio ;
- Via Sant'Iffredo – Centro Anziani CAM2 per finalità di tutela della sicurezza urbana e tutela del patrimonio;
- Piazza Giovanni Paolo II per finalità di tutela della sicurezza urbana;
- Viale Salmatoris per finalità di tutela della sicurezza urbana;
- Corso L. Einaudi per finalità di tutela della sicurezza urbana;

- Via Moglia – Discesa Nuova per finalità di tutela della sicurezza pubblica;
- Via Discesa Vecchia per finalità di tutela della sicurezza urbana;
- Fraz. Roreto di Cherasco – Piazza adiacente via Cuneo – Raccolta Verde per finalità di tutela della sicurezza urbana e tutela ambientale;
- Fraz. Roreto di Cherasco – Piazza Caduti CAM1 per finalità di tutela della sicurezza urbana;
- Fraz. Roreto di Cherasco – Piazza Caduti CAM2 per finalità di tutela della sicurezza urbana;
- Fraz. Roreto di Cherasco – Via Rimembranze per finalità di tutela della sicurezza urbana;
- Fraz. Roreto di Cherasco – Rotatoria S.P. 662/ S.S. 231 per finalità di tutela della sicurezza urbana e per lettura targhe;
- Fraz. San Michele CAM1 per finalità di tutela della sicurezza urbana;
- Fraz. San Michele CAM2 per finalità di tutela della sicurezza urbana;
- Fraz. Bricco de Faule – Via Fossano per finalità di tutela della sicurezza urbana;
- Fraz. Bricco de Faule – Giardini Pubblici Via Fossano per finalità di tutela della sicurezza urbana;
- Fraz. Bricco de Faule – Via Fossano zona Cimitero per finalità di tutela della sicurezza urbana;
- Fraz. Bricco de Faule – Piazza Asilo adiacente Via Fossano per finalità di tutela della sicurezza urbana;
- Fraz. Veglia CAM1 per finalità di tutela della sicurezza urbana;
- Fraz. Veglia CAM2 per finalità di tutela della sicurezza urbana;
- Fraz. Veglia CAM3 per finalità di tutela della sicurezza urbana;
- Fraz. Cappellazzo CAM1 per finalità di tutela della sicurezza urbana;
- Fraz. Cappellazzo CAM2 per finalità di tutela della sicurezza urbana;
- Fraz. Picchi CAM1 per finalità di tutela della sicurezza urbana;
- Fraz. Picchi CAM2 per finalità di tutela della sicurezza urbana;
- Fraz. Picchi CAM3 per finalità di tutela della sicurezza urbana;
- Fraz. San Bartolomeo per finalità di tutela della sicurezza urbana;
- Loc. Bernocchi per finalità di tutela della sicurezza urbana.

Accanto a tale impianto di telecamere Il Comune di Cherasco, al fine di contrastare, scoraggiare e prevenire l'increscioso abbandono e smaltimento illecito dei rifiuti sul territorio, nonostante i numerosi controlli ambientali effettuati dalla Polizia Municipale, si avvale di un sistema di videosorveglianza realizzato mediante l'utilizzazione di fototrappole collocate, per un determinato tempo, in prossimità dei siti maggiormente a rischio (lungo le strade, e nelle loro pertinenze nonché nelle aree verdi).

Le fototrappole sono progettate per l'uso all'aperto e si innescano a seguito di qualsiasi movimento di essere umani o animali monitorata da un sensore ad alta sensibilità di movimento a infrarossi passivo, per poi scattare foto e video clip.

Il **titolare del trattamento:** è il Comune di Cherasco Via Vittorio Emanuele n° 79 12062 Cherasco (CN) - Telefono: +39 0172./427010 Fax: +39 0172/427016 email: urp@comune.cherasco.cn.it PEC: chersco@postemailcertificata.it

Il responsabile della protezione dati: è il Dr. Luigi MAZZARELLA Via Marconi n° 55 12042 - BRA (CN) - Telefono: +347 7445568, email: pmazzarella@tiscali.it PEC: pmazzarella@postecert.it

Il responsabile del trattamento: è S.T. S.r.l." di Udine, con sede in Viale Tricesimo, n.184/3; Tel. 800 939310., email: info@gruppost.it - aministrazione@gruppost.it

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 della polizia urbana 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 in condizioni di sufficiente illuminazione naturale o artificiale, o, in caso contrario in bianco/nero.

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

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

Mentre le immagini fotografiche o video riprese dalle fototrappole sono trasferite su di un portale 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 forze dell'ordine

Eventuali accessi di persone diverse da quelli innanzi indicate sono autorizzati per iscritto, 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 permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

L'accesso alle immagini da parte del designato edi prposti si limita alle attività oggetto della 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'intera durata 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 è necessario 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 dei dati 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 espressa e motivata disposizione dell'Autorità giudiziaria.

Designato al Trattamento è: Perano Livio–Responsabile del servizio di Polizia Locale

Preposti al trattamento sono:

- Baudissone Mirko
- Busso Marco
- Martinengo Germano
- Trucco Marco

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

Quali sono le risorse di supporto ai dati?

Il dato delle immagini è conservato su NVR server su cui è trasmesso via radio dalla telecamera, quest'ultima appunto, trasmette le informazioni e le immagini via radio o via collegamento in fibra ottica al server Milestone.

Mentre il dato di rilevazione delle targhe è conservato su di un P.C. Windows. 10

Il sistema di registrazione è stato dimensionato per esaltare le performance di registrazione, supervisione e fruizione del registrato.

Il server è equipaggiato con n. 4 (QUATTRO) dischi in raid, n. 5 (CINQUE) per lo storage delle immagini e di n. 2 (DUE) SSD per il sistema operativo, processore Intel Weon.

Il link radio si basa sulla tecnologia "punto-punto" o "punto multi punto" realizzati con tecnologia 5GHZ a frequenza libera, criptatura della componente radio con protocollo WPA2/Personal e protezione mediante password dei parametri di configurazione della radio.

Mentre i dati registrati nelle schede SD delle fototrappole sono crittografati e protetti da un codice di protezione, in modo da evitare la consultazione non autorizzata da parte di estranei.

In casi di furto delle fototrappole dovrà essere effettuata da remoto la cancellazione di tutti i dati memorizzati all'interno della scheda SD.

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 che fanno parte della comunita;
- 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 strumenti e 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 sacrificio del 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 in luoghi 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 Cherasco, con deliberazione n. 73/CC.. adottata in data 19/12/2019 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 finalità possono 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 la modifica.

Qual è il periodo di conservazione dei dati?

Le immagini registrate sono conservate per il tempo necessario per le finalità per le quali 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 delle immagini 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 in cui 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 Garante per 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 periodo di 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 e dalle linee guida dell'"Europen Data Protection Board" - edpb - del 3/2019 sul trattamento dei dati personali attraverso dispositivi videosorvegliana

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.

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 dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e 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, con un anticipo di giorni dieci.

Relativamente alla videosorveglianza per il controllo della sicurezza stradale l'informativa è 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 di un 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 dei dati?

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 designato del trattamento, senza ritardo e comunque non oltre 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 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), 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 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 o comunicata oralmente, che dovrà provvedere in 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 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 Designato 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.

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 per la protezione dei dati personali (Data Protection Office, DPO), secondo quanto indicato al precedente 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 una protezione 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, 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 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 manutenzione compiuta 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 del personale 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 interrompere il 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'IP pubblico 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 ritualmente nominati.

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 lettura delle 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.

Ha proceduto ad uno specifico corso di formazione per il personale dipendente

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L'ente ha predisposto una procedura operativa interna per la gestione di un eventuale data breach, cosi come previsto dal Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni 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 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.

Nella sede municipale sono presenti n. 2 estintori, 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 hacher , 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 - Hacher

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 ricerca mirata 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 alle minacce, alle fonti di rischio e alle misure pianificate?
Trascurabile.

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.

Il server, per la parte della videosorveglianza non è collegato ad internet (riducendo drasticamente, quindi, la già scarsissima probabilità di attacco informatico esterno) e le telecamere trasmettono le immagini con segnale radio crittografato.

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

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).

La presenza di un log eventi consente di monitorare ogni accesso, tenendo così traccia anche degli accessi illeciti e non motivati. I log eventi è controllato periodicamente proprio a tal fine.

L'asportazione fisica dei supporti di memorizzazione è una azione che ha anch'essa una probabilità di verificazione del tutto irrisoria: i locali che ospitano tali supporti sono inaccessibili da chiunque non sia in possesso di apposita chiave di accesso in quanto chiusi in un locale adibito *ad hoc*.

Il monitor per la visualizzazione in diretta delle immagini è sito in posizione tale da non essere visibile al pubblico, evitando così che chiunque possa visionare le immagini.

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 del rischio?

Attacco da remoto ai sistemi da parte di hacher , 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 no adeguatamente preparato Fonti umane esterne - Hacher

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 dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della 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 e delle misure pianificate?

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.

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'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.

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 reato subito, Percezione di insicurezza

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

Attacco da remoto, Accesso non autorizzati alla sala di controllo, Malfunzionamenti fisici dei sistemi, Eventi naturalistici

Quali sono le fonti di rischio?

Fonti umane interne, - Personale no adeguatamente preparato Fonti umane esterne - Hacher

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 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

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, 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 alle modeste 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 apparati tecnici.

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 Cherasco è sito in zona 3.

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 diversa tecnologia

Cherasco lì 23/11/2021

Il Titolare del trattamento
Comune di Cherasco

Il Data Protection Officer
Mazzarella dott.re Luigi