Unione Comunale dei Colli

Data Protection Impact Assessment

Sul trattamento dei dati effettuato per la gestione del sistema integrato di videosorveglianza

Versione 1.3 (18.11.2022)

Redatta da: Dott. Fabio Masserini

Verificata da: Ing. Gianpietro Turani

Validata da: Dott. Mattia Cortinovis

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

I trattamenti oggetto della DPIA sono quelli relativi al sistema di videosorveglianza integrato realizzato dall'Unione Comunale dei Colli.
Le componenti specifiche sono:

- il sistema di videosorveglianza tradizionale;
- le fototrappole;
- il sistema di lettura targhe;
- il sistema di rilevamento automatico della velocità;
- le dashcam in dotazione alle auto di servizio della polizia locale;
- in prospettiva, le bodycam in dotazione degli agenti di polizia locale (attualmente non ancora acquisite, in corso di valutazione).

La finalità del trattamento è quella di tutelare più efficacemente la sicurezza sul territorio tramite strumenti di videosorveglianza integrata.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento è l'Unione Comunale dei Colli.
Contitolari del trattamento sono i diversi comuni che compongono l'Unione.
Suardi Srl di Chiuduno è responsabile esterna del trattamento poiché fornisce un servizio di assistenza informatica e sistemistica sul sistema di videosorveglianza.
Engine S.r.l. è responsabile esterna del trattamento poiché fornitrice del sistema di rilevamento automatico della velocità

Ci sono standard applicabili al trattamento?

Regolamento UE 2016/2016;
Direttiva UE n. 2016/680 del 27 aprile 2016 relativa 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
Decreto Legislativo 10 agosto 2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", che modifica e integra il d.lgs. 196/2003 Codice nazionale sulla privacy";
Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";

Decreto Legislativo 18 maggio 2018, n. 51/2018 “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”;
Provvedimento del Garante per la Protezione dei Dati personali in materia di videosorveglianza 8 aprile 2010;
Linee guida EDPB n. 3/2019 sul trattamento di dati personali attraverso dispositivi video Versione 2.0 adottate il 29 gennaio 2020
Regolamento sulla videosorveglianza approvato con deliberazione dell’Assemblea dell’Unione n. 9 del 22.07.2021

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

- I dati oggetto di trattamento sono le riprese video effettuate dalle telecamere fisse e mobili, dalle telecamere per il rilevamento delle targhe e della velocità, nonché delle fototrappole, dalle dashcam e (in prospettiva) dalle bodycam. Sono inoltre trattati i metadati (numero di targa, orario e luogo di passaggio) registrati dal sistema di lettura targhe.
- Il tempo di conservazione delle immagini è di 7 giorni. I metadati vengono invece conservati per un anno. Nel caso in cui dei dati specifici debbano essere utilizzati nell’ambito di indagini o procedimenti amministrativi, vengono estratti e conservati per il maggior periodo necessario (fino al termine dell’indagine/procedimento).
- I destinatari potenziali dei dati sono le autorità di polizia e/o giudiziarie, nel caso in cui le immagini riprese o i metadati diano l'avvio a (o siano utilizzati nell'ambito di) indagini.
- Le persone che possono accedere ai dati sono gli addetti della polizia locale a ciò espressamente autorizzati dal Comandante, nonché i sindaci dei singoli comuni facenti parte dell’Unione (ciascuno limitatamente al territorio di propria competenza). Possono inoltre accedere ai dati, esclusivamente per finalità di supporto tecnico, i responsabili esterni.
  È in corso di valutazione la condivisione dei dati registrati dal sistema di rilevamento targhe con i comandi provinciali dell’Arma carabinieri, della Questura e Guardia di finanza, con i quali dovrà essere stipulata un’apposita convenzione.

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

SISTEMA DI VIDEOSORVEGLIANZA TRADIZIONALE:

- il dato viene raccolto tramite telecamere di osservazione di tipo fisso o brandeggiabile, dotate di protezioni varie:
  - collocazioni non facilmente accessibili;
  - configurazioni protette da password;
  - assenza di registrazioni decentrate (cioè assenza di dispositivi di memorizzazione prossimi alla telecamera stessa);
- i flussi video sono convogliati verso i server di videosorveglianza (posizionati nei comuni dell’unione) attraverso infrastruttura apposita (tecnologia radio Hiperlan);
- i flussi sono raccolti dai server di videosorveglianza; le immagini sono visionabili, attraverso software apposito, solo da personale autorizzato:

    - il sindaco dello specifico comune ha accesso alle immagini generate dalla propria infrastruttura di videosorveglianza;
    - il comando di polizia locale (e gli utenti ivi autorizzati) accedono a tutti i server di video sorveglianza di ogni comune dell'Unione attraverso VPN;
- i dati vengono conservati sul server per 7 giorni; dopo tale lasso di tempo vengono automaticamente cancellati, fatta eccezione per i dati esportati e salvati separatamente per accertamenti in corso.

SISTEMA DI LETTURA TARGHE:

- il dato viene raccolto tramite telecamere OCR, dotate di protezione contro accessi indesiderati (collocazioni inaccessibili);
- il flusso video e i metadati correlati sono convogliati verso la centrale di lettura targhe (polizia locale) attraverso rete mobile (si impiegano SIM dell'operatore TIM);
- i flussi sono raccolti dal server di lettura targhe e resi disponibili agli utenti abilitati all'accesso tramite opportuna autenticazione;
- i dati raccolti sono anche trasmessi in tempo reale ai tablet in dotazione agli agenti di polizia locale in corrispondenza dei varchi che sono oggetto del loro presidio e limitatamente ai veicoli per i quali il sistema centrale ha rilevato irregolarità;
- i dati di immagine vengono conservati sul server per 7 giorni; dopo tale lasso di tempo vengono automaticamente cancellati, fatta eccezione per i dati esportati e salvati separatamente per accertamenti in corso;
- i metadati (ai quali può accedere solo il comandante della polizia locale) sono invece conservati per un anno;
- in passato i dati erano resi direttamente accessibili anche alle autorità di polizia giudiziaria (comandi provinciali carabinieri, Questura, guardia di finanza e altri comandi delle ff.pp. della provincia e fuori provincia). Tale condivisione è stata interrotta per valutare le corrette modalità con cui i dati possano essere resi accessibili a tali autorità: è in corso la valutazione di un'apposita convenzione volta a regolare la materia;
- il sistema di lettura targhe presentava un'apertura verso il sistema Interforze; quest'ultimo poteva introdurre nel sistema di lettura targhe una black-list di targhe sulla base della quale Interforze era allertata a fronte del passaggio nei varchi dell'Unione di un veicolo corrispondente alle informazioni in black-list; la polizia locale non era coinvolta e non interferiva in questo tipo di indagini; da ottobre 2022 l'apertura verso Interforze è stata disattivata in attesa di regolare correttamente i rapporti tra il Titolare e i soggetti esterni coinvolti.

SISTEMA DI RILEVAMENTO AUTOMATICO DELLA VELOCITÀ:

- il dato viene raccolto tramite telecamere OCR, dotate di protezione contro accessi indesiderati;
- il flusso video e i metadati correlati sono convogliati verso un server dedicato (è utilizzata la trasmissione con SIM di operatore mobile); i dati sono salvati solo se pertinenti per la contestazione di contravvenzioni relative al superamento dei limiti di velocità;
- i flussi sono raccolti dal server e resi disponibili agli utenti abilitati all'accesso (agenti della polizia locale) tramite opportuna autenticazione;
- i dati raccolti, previo controllo da parte di un operatore di polizia, vengono usati per la contestazione di eventuali sanzioni relative al superamento dei limiti di velocità;
- i dati sono conservati fino al termine del procedimento sanzionatorio.

FOTOTRAPPOLE:

- il dato viene raccolto tramite fototrappole collocate nei punti di osservazione definiti;
- i dati vengono salvati sulla scheda di memoria localizzata all'interno della fototrappola; l'accesso alla scheda e alla fototrappola è protetto da un contenitore di sicurezza dotato di serratura;
- i dati vengono prelevati dalla fototrappola dopo che questa è stata portata da personale addetto presso la sede della polizia locale per l'estrazione dei dati e/o il cambio della batteria;
- le immagini presenti sulla scheda di memoria contenuta nella fototrappola sono quindi esaminate dagli agenti autorizzati e vengono cancellate salvo il caso in cui si renda necessaria la loro conservazione ulteriore per finalità di indagine o di accertamenti amministrativi; in tale ipotesi vengono invece archiviate su PC dedicato con accesso protetto tramite username e password.

DASHCAM:

- le dashcam sono in dotazione delle automobili di servizio della polizia locale e vengono attivate dagli agenti che le utilizzano;
- i dati vengono salvati sulla scheda di memoria localizzata all'interno della dashcam stessa; la scheda di memoria viene continuamente sovrascritta, cancellando i dati precedenti;
- le registrazioni vengono scaricate e salvate dal comandante della polizia locale nel caso in cui si renda necessaria la loro visione e conservazione ulteriore per finalità di indagine o di accertamenti amministrativi; in tale ipotesi vengono invece archiviate su PC dedicato con accesso protetto tramite username e password; gli agenti non sono autorizzati ad accedere alle informazioni registrate dalle dashcam.

BODYCAM:

- è in corso di valutazione l'adozione di bodycam per facilitare le operazioni di polizia locale e promuovere la sicurezza delle persone attenzionate da un'attività di polizia e degli stessi agenti;
- le bodycam verranno assegnate dal comandante della polizia locale agli agenti che potrebbero averne necessità in base alle mansioni svolte;
- le bodycam verranno attivate dagli agenti che le utilizzano nelle occasioni e con le modalità previste da un apposito regolamento predisposto dal Comandante;
- i dati registrati dalle bodycam saranno salvati nella scheda di memoria interna;
- le registrazioni verranno scaricate e salvate dal comandante della polizia locale nel caso in cui si renda necessaria la loro visione e conservazione ulteriore per finalità di indagine o di accertamenti amministrativi; in tale ipotesi verranno archiviate su PC dedicato con accesso protetto tramite username e password.

Quali sono le risorse di supporto ai dati?

Hardware / Sistemi operativi / RAM-CPU / Client

SISTEMA DI LETTURA TARGHE:

- Server Polizia Locale:
    - Hardware: Fujitsu PRIMERGY RX2520 M1 - 2 HDD da 300 GB in RAID 1 - 1 HDD da 2 Tb in RAID 0

    - Sistema Operativo: Windows Server 2012 R2 Standard - Processore Intel Xeon CPU E5-2407 v2 2.40 GHZ - RAM 8 GB
    - CPU-RAM
        - Xeon con 8 GB di RAM
    - Software
        - CPS Selea
- Telecamere sul territorio
    - modelli Vigilate v-Plate
    - modelli Selea

SISTEMI DI VIDEOSORVEGLIANZA:

- Server
    - Hardware
        - Fujitsu PRIMERGY (RX2520)
        - Dell PowerEdge (T440, R530)
    - Sistemi operativi dei server
        - Windows Server 2019
    - CPU-RAM server
        - Xeon con 8/16 GB di RAM a seconda dei casi
    - Software
        - Milestone System
- Telecamere (vari modelli)
    - Hikvision
    - Dahua
    - Panasonic

SISTEMA DI FOTOTRAPPOLE:

- Sistema operativo a bordo del dispositivo fototrappola che supporta la configurazione completa del dispositivo (parametri di raccolta immagini, parametri del sensore a infrarossi, configurazione della scheda di memoria inserita).

Reti:

Infrastruttura di rete mista:

- Cablata: in fibra ottica
- Wireless in tecnologia Hiperlan (HIgh PErformance Radio LAN) su frequenza libera 5 Ghz;
- 4G.

Persone:

Possono accedere ai dati trattati nell'ambito del sistema di videosorveglianza solo gli agenti della polizia locale dell'Unione Comunale dei Colli a ciò espressamente autorizzati dal comandante, con nomina scritta e assegnazione di credenziali nominative univoche. I sindaci dei singoli Comuni, inoltre, possono accedere alle immagini del sistema di videosorveglianza tradizionale limitatamente alle immagini del proprio territorio.

Il trattamento dei dati è svolto solo dal comandante della polizia locale per quanto concerne:

- La visione e l'estrazione e la conservazione delle immagini registrate da dashcam ed eventualmente bodycam;

- la visione e la conservazione dei metadati del sistema di lettura targhe.

Per necessità occasionali di manutenzione del sistema potrebbero inoltre accedere ai dati gli incaricati delle ditte che erogano tale servizio, regolarmente nominate come responsabili esterne del trattamento.

Valutazione: Da correggere

Con riferimento alle dashcam, il salvataggio di dati non crittografati e potenzialmente accessibili a chiunque abbia accesso fisico alle telecamere e strumenti idonei per collegarsi alle stesse comporta un rischio di perdita di riservatezza, integrità e disponibilità dei dati. Occorre introdurre un sistema che limiti la possibilità di accesso, modifica e cancellazione dei dati ai soli soggetti dotati di apposite credenziali.

Inoltre, la mancata definizione di procedure per il periodico controllo/salvataggio/cancellazione delle immagini comporta un rischio per la disponibilità dei dati, che potrebbero essere cancellati prematuramente ove le registrazioni siano mantenute attive per periodi più lunghi del previsto. Occorre introdurre un sistema che consenta di determinare con sicurezza il tempo di conservazione del dato.

I server di videosorveglianza collocati nei comuni dell'Unione non sono posizionati e gestiti nel rispetto di idonee policy di sicurezza fisica: occorre posizionare tutti i server in luoghi sicuri.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono specifici ed espliciti, consistendo nella facilitazione delle attività di polizia amministrativa e polizia giudiziaria.

Tali scopi sono legittimi poiché conformi a quanto previsto dalla L. 7/3/1986, n. 65 e dalla L. R. n. 6/2015.

Quali sono le basi legali che rendono lecito il trattamento?

La base legale è l'interesse pubblico a realizzare la suddetta finalità di facilitazione delle attività di polizia amministrativa e polizia giudiziaria., nell'ambito della cornice normativa fornita dalla L. 7/3/1986, n. 65 e dalla L. R. n. 6/2015.

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

I dati raccolti sono adeguati e pertinenti rispetto alle finalità del trattamento: le riprese hanno infatti un'utilità specifica e dimostrata nel facilitare le attività facilitazione delle attività di polizia amministrativa e polizia giudiziaria.

Non sono acquisiti dati ulteriori rispetto a quelli strettamente necessari per il perseguimento delle finalità: le registrazioni (eccetto quelle eventualmente fatte tramite bodycam) non includono l'audio.
I dati rilevati dal sistema di rilevamento automatico della velocità non sono salvati salvo quando necessari per contestare violazioni dei limiti di velocità.

I dati sono esatti e aggiornati?

L'esattezza e l'aggiornamento dei dati sono garantiti dalla tipologia di dati trattati (riprese video), e dall'utilizzo di sistemi di ripresa tecnologicamente aggiornati.

Qual è il periodo di conservazione dei dati?

Il periodo di conservazione delle immagini è generalmente di 7 giorni, come previsto dall'art. 6, comma 8, del DL n. 11/2009 e dal Provvedimento del Garante dell'8 aprile 2010.
Le immagini registrate dal sistema di videosorveglianza tradizionale sono cancellate automaticamente al termine del periodo di conservazione, mediante sovrascrittura delle registrazioni precedenti.
Per quanto riguarda specificamente le fototrappole, a causa di esigenze tecniche la cancellazione avviene manualmente a cura degli operatori autorizzati.
Per quanto riguarda specificamente le dashcam, le immagini sono conservate fino alla sovrascrittura dovuta all'esaurimento dello spazio di memoria.
Per quanto riguarda il sistema di lettura targhe, i metadati (targa, orario e luogo del passaggio) sono conservati per un anno.
Le riprese che eventualmente attestino la commissione di illeciti penali o amministrativi possono essere copiate e conservate fino al termine delle indagini e dei procedimenti sanzionatori che ne conseguono.

Valutazione: Da correggere

Con riferimento alle dashcam, l'attivazione delle registrazioni non va lasciata all'iniziativa dei singoli agenti ma dovrebbe essere disciplinata da un apposito regolamento o mediante istruzioni impartite dal Titolare.
Con riferimento alle dashcam, la cancellazione dei dati tramite sovrascrittura non risulta sufficiente perché dipende dal loro effettivo utilizzo, e potrebbe quindi portare a una conservazione eccessivamente prolungata; occorre introdurre procedure per assicurare che i dati siano in ogni caso cancellati a scadenze determinate (ogni 7 giorni).
Con riferimento alle fototrappole, occorre introdurre procedure per assicurare che i dati siano in ogni caso cancellati a scadenze determinate (ogni 7 giorni).
Con riferimento al sistema di lettura targhe, il periodo di conservazione dei metadati (un anno) risulta sproporzionato rispetto alle finalità del trattamento, e andrebbe ridotto.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

L'informativa è fornita in modalità completa mediante un'apposita pagina web pubblicata dall'Unione Comunale dei Colli.

Alla cittadinanza vengono inoltre fornite informative brevi mediante l'affissione di appositi cartelli nelle zone dove sono poste le telecamere del sistema di videosorveglianza tradizionale, del sistema di lettura targhe e del sistema di rilevamento della velocità. Analoghi cartelli sono esposti nelle zone dove vengono temporaneamente poste le fototrappole.

Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile poiché il trattamento non è fondato sul consenso degli interessati.

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

Il diritto di accesso è disciplinato dall'art. 19 del Regolamento sulla videosorveglianza. Gli interessati possono ottenere l'accesso solo a riprese che li riguardano, e a tal fine dovranno specificare il luogo delle riprese, l'orario indicativo, le attività in corso e il vestiario indossato. L'istanza è gestita e valutata dal Designato del trattamento a ciò preposto (il Comandante della Polizia Locale), che provvede a individuare le riprese pertinenti e, se necessario, a rendere irriconoscibili le immagini di eventuali soggetti terzi.
Il diritto di portabilità non risulta applicabile poiché non ricorrono i presupposti individuati dalla normativa per il suo esercizio da parte degli interessati.

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

Il diritto di rettifica non è applicabile date le caratteristiche tecniche del trattamento.
Il diritto di cancellazione appare di residuale applicabilità, data la tipologia di trattamento e data la cancellazione delle immagini trascorso il periodo di conservazione; in ogni caso può essere esercitato contattando il Titolare ai recapiti indicati nell'informativa privacy pubblicata sul sito dei titolari del trattamento.

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

Il diritto di limitazione e di opposizione appare di residuale applicabilità, data la tipologia di trattamento e data la cancellazione delle immagini trascorso il periodo di conservazione; in ogni caso possono essere esercitati contattando il Titolare ai recapiti indicati nell'informativa privacy pubblicata sul sito dei titolari del trattamento.

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

I responsabili del trattamento (alla data di conduzione della DPIA, con possibili variazioni future dovute al subentro di altri fornitori) sono:

- Suardi Srl di Chiuduno, che si occupa della gestione tecnica e della manutenzione dei sistemi di videosorveglianza tramite telecamere fisse e di lettura targhe.
- Engine S.r.l., che fornitrice del sistema di rilevamento automatico della velocità

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

Non applicabile, poiché non sono effettuati trasferimenti dei dati fuori dall'Unione Europea.

Valutazione: Da correggere

Con riferimento alle dashcam, occorre fornire un'informativa breve agli interessati, ad esempio esponendola sulle auto di servizio che sono dotate dello strumento.
Con riferimento ai sistemi di videosorveglianza tradizionale, di lettura targhe e di rilevamento automatico della velocità, è opportuno verificare la completezza della cartellonistica esposta.
Con riferimento alle fototrappole, è opportuno formalizzare delle istruzioni agli operatori sul posizionamento dei cartelli volti a fornire l'informativa breve.

Misure di sicurezza

Misure esistenti o pianificate

Crittografia
La crittografia è implementata sui server e sulle schedine SD presenti nelle telecamere come memoria tampone.
Valutazione: Migliorabile
Piano d'azione / misure correttive:
Estendere l'impiego di crittografia, ove possibile, anche ai client che si interfacciano con i vari sistemi di videosorveglianza in modo che le informazioni estratte in locale non siano facilmente carpibili.
Commento di valutazione:
La crittografia non è implementata su tutti i sistemi client.

Formazione
Strumenti di formazione sulla normativa privacy sono stati messi a disposizione del Designato e degli autorizzati
Valutazione: Migliorabile
Piano d'azione / misure correttive:
È opportuno definire un piano di formazione che includa iniziative periodiche di sensibilizzazione e miglioramento.
Commento di valutazione:
Viene offerta formazione sulla normativa privacy ma non con modalità sistematiche e pianificate.

Controllo degli accessi logici
Il controllo è effettuato tramite utenze nominative, ciascuna profilabile con diversi livelli di autorizzazione
Valutazione: Accettabile

Tracciabilità
Viene tracciato per sei mesi tramite appositi log l'accesso degli operatori che visualizzano le immagini o svolgono qualsiasi altra operazione sui dati. Non vengono tracciate le operazioni svolte (download, eventuali modifiche) sui server di videosorveglianza dai vari operatori che si collegano.
Valutazione: Migliorabile
Piano d'azione / misure correttive:
Valutare la possibilità di aumentare la tracciatura delle azioni compiute dagli operatori sui vari sistemi di videosorveglianza.
Commento di valutazione:
Si segnala l'opportunità di aumentare la tracciatura delle azioni svolte.

Archiviazione
Videosorveglianza: svolta in locale e su NAS in prossimità, per un periodo massimo di 7 giorni. Lettura targhe: svolta in locale tramite un server dedicato, per un periodo massimo di 7 giorni (immagini) e un anno (metadati).

L'archiviazione è ad alta affidabilità (dischi in RAID0/RAID1/RAID5).
Valutazione: Accettabile

Vulnerabilità
Aggiornamento periodico manuale sui sistemi operativi dei server.
Valutazione: Accettabile
Commento di valutazione:
I sistemi operativi dei server sono aggiornati (Windows 2019). Il sistema operativo del sistema di lettura targhe è Windows 2012 R2 (fine supporto ottobre 2023).

Lotta contro il malware
Sui server sono installati gli antivirus Webroot e Microsoft (integrato nel sistema operativo). In un caso specifico l'antivirus non è presente.
Valutazione: Da correggere
Piano d'azione / misure correttive:
Occorre provvedere all'installazione di software antivirus professionali su tutti i server ove sono custodite le registrazioni delle immagini.

Gestione postazioni
Le postazioni sono protette tramite utenze nominative di rete.
Valutazione: Accettabile

Sicurezza dei siti web
I dati non transitano da siti web pubblici.
Valutazione: Accettabile

Backup
Non viene effettuato un backup remoto dei dati in quanto si dispone di robusti dispositivi di storage a bordo del server e in prossimità (NAS).
Valutazione: Migliorabile
Piano d'azione / misure correttive:
Valutare l'introduzione di un sistema di backup remoto per i dati critici.

Manutenzione
La manutenzione viene effettuata a cura di Suardi Srl di Chiuduno (responsabile esterna del trattamento).
Valutazione: Accettabile

Contratto con il responsabile del trattamento
I contratti con i responsabili del trattamento soddisfano i requisiti e contengono le garanzie richieste dall'art. 28 del GDPR.
Valutazione: Accettabile

Sicurezza dei canali informatici
L'accesso ai dati di videosorveglianza comunali da parte del comando dei vigili avviene mediante VPN.

La trasmissione dei dati dalle telecamere (di videosorveglianza e lettura targhe) ai server avviene tramite rete mista:

- Cablata: in fibra ottica
- Wireless in tecnologia Hiperlan (HIgh PErformance Radio LAN) su frequenza libera 5 Ghz;
- 4G.

Valutazione: Accettabile

Controllo degli accessi fisici

Il server di lettura targhe è custodito in un locale dedicato presso la sede della polizia locale.
I server di videosorveglianza sono custoditi presso i comuni, ma in alcuni casi in locali promiscui ad accesso non protetto.
Valutazione: Migliorabile
Commento di valutazione:
Si rinvia al termine del paragrafo “Quali sono le risorse di supporto ai dati?”, a pagina 7.

Sicurezza dell'hardware

I server sono custoditi in locale dotato di condizionatore. I server sono protetti da dispositivi UPS.
Valutazione: Adeguato

Gestione dei terzi che accedono ai dati

L'accesso ai dati comunali di videosorveglianza da parte del comando avviene mediante VPN su rete dedicata. Analogamente gli accessi da parte della società Suardi Srl di Chiuduno per le varie attività di manutenzione.
Valutazione: Accettabile

Rischi

Accesso illegittimo ai dati

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

- L'accesso e la diffusione illegittima dei dati potrebbero comportare danni reputazionali per gli interessati, nel caso di riprese che li riguardano e che li vedono coinvolti in attività compromettenti
- Un sistematico accesso abusivo da parte di soggetti esterni potrebbe essere utilizzato per attività di stalking o per determinare la posizione dell'interessato, al fine di commettere reati a suo danno
- Il sistema di videosorveglianza potrebbe essere utilizzato dalle forze di polizia (o da altri soggetti interni al Comune) per svolgere indagini o attività di sorveglianza abusive nei confronti di determinati interessati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Attacco informatico finalizzato alla sottrazione dei dati

- Errore tecnico nell'attribuzione di permessi (eccessivi) agli autorizzati
- Sottrazione manuale dei dati o accesso abusivo da parte di autorizzati infedeli

Quali sono le fonti di rischio?

- Fonti umane esterne - criminali informatici
- Fonti umane interne - amministratori di sistema, designati, responsabili o autorizzati negligenti
- Fonti umane interne - amministratori di sistema, designati, responsabili o autorizzati infedeli

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Crittografia
- Formazione
- Tracciabilità
- Controllo degli accessi logici
- Gestione postazioni
- Lotta contro il malware
- Controllo degli accessi fisici
- Sicurezza dell'hardware

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

Limitata.

Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà.

Le riprese vengono effettuate esclusivamente in luoghi pubblici o aperti al pubblico e per bodycam, in attività specifiche di polizia, anche in luoghi privati: pertanto non vi è una particolare aspettativa di riservatezza da parte degli interessati, i quali sono consapevoli del fatto che le attività poste in essere potrebbero essere viste da chiunque sia presente in loco.

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

Limitata.
In generale, la probabilità risulta limitata date le stringenti misure di sicurezza e di controllo degli accessi adottate dal Titolare.
Le credenziali di accesso sono nominative, e possono essere assegnate solo dal Designato del trattamento (il Comandante della Polizia Locale) a soggetti che ne abbiano un'effettiva necessità per lo svolgimento delle proprie mansioni. L'art. 7 del Regolamento di videosorveglianza prevede inoltre una rigorosa profilazione delle utenze, che saranno tecnicamente limitate a svolgere solo le operazioni di propria competenza (mera consultazione, estrazione di copia delle immagini, cancellazione, modifica delle inquadrature, ecc.).
I soggetti interni autorizzati a trattare i dati, inoltre, sono pubblici ufficiali formati sui propri obblighi e soggetti a sanzioni elevate in caso di comportamenti abusivi, ciò che riduce ulteriormente la probabilità di comportamenti dolosi in violazione della riservatezza dei dati.

L'accesso da parte di esterni è invece improbabile data la significativa difficoltà di superare le misure di sicurezza, combinata con la scarsa utilità che un criminale informatico potrebbe trarre dai dati, da cui consegue la mancanza di particolari incentivi.

Tuttavia, con riferimento specifico alle dashcam, il livello di rischio è aumentato dalla carenza di sistemi di controllo degli accessi alle schede di memoria. Le dashcam e le relative schede di memoria sono comunque custodite all'interno delle automobili della polizia locale, ciò che implica un controllo dell'accesso fisico ai dispositivi.
Inoltre, con riferimento al sistema di lettura targhe l'eccessivo periodo di conservazione dei metadati comporta un aumento del rischio di perdita di riservatezza dei dati stessi.
Per maggiori dettagli si rinvia alle valutazioni formulate ai paragrafi precedenti.

Valutazione: Da correggere

Si rinvia alle valutazioni formulate ai paragrafi precedenti.

Modifiche indesiderate dei dati

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

- La corruzione dei dati potrebbe comportare l'impossibilità per l'interessato di usare le registrazioni a dimostrazione della propria estraneità rispetto alla commissione di illeciti penali, civili o amministrativi, o come prova a carico di terzi qualora l'interessato sia una parte lesa.
- L'alterazione dolosa delle immagini potrebbe consentirne l'utilizzo come falsa prova a carico dell'interessato

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

- Corruzione dei file durante la trasmissione dei dati dalle telecamere ai server
- Mancata trasmissione dei dati immagine dalle telecamere ai server
- Intervento doloso di manipolazione delle immagini registrate
- Corruzione dei file durante la conservazione su server

Quali sono le fonti di rischio?

- Fonti umane esterne - criminali informatici
- Fonti non umane - malfunzionamenti tecnici degli impianti che causino la corruzione delle immagini
- Fonti umane interne - amministratori di sistema, designati, responsabili o autorizzati negligenti
- Fonti umane interne - amministratori di sistema, designati, responsabili o autorizzati infedeli

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

- Formazione
- Tracciabilità
- Archiviazione
- Lotta contro il malware
- Manutenzione
- Sicurezza dell'hardware

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

Importante.
In casi estremi di alterazione delle immagini (particolarmente se dolosa) gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.
Il rischio peggiore riguarda le ipotesi in cui le immagini alterate non possano essere utilizzate come prova a favore dell'interessato, o viceversa possano essere utilizzate come prova a suo carico.

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

Limitata.
In generale, la probabilità di un'alterazione colposa dei dati è limitata, date le misure di sicurezza e le caratteristiche tecniche dell'impianto.
La probabilità di un'alterazione dolosa è trascurabile, data la difficoltà di realizzarla combinata alle scarse possibilità per l'eventuale responsabile di trarne un vantaggio effettivo.
Tuttavia, con riferimento specifico alle dashcam, il livello di rischio è aumentato dalla carenza di sistemi di controllo degli accessi. Le dashcam e le relative schede di memoria sono comunque custodite all'interno delle automobili della polizia locale, ciò che implica un controllo dell'accesso fisico ai dispositivi.

Valutazione: Da correggere

Si rinvia alle valutazioni formulate ai paragrafi precedenti.

Perdita di dati

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

- La perdita dei dati potrebbe comportare l'impossibilità per l'interessato di usare le registrazioni a dimostrazione della propria estraneità rispetto alla commissione di illeciti penali, civili o amministrativi, o come prova a carico di terzi qualora l'interessato sia una parte lesa.

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

- Attacchi informatici esterni non mirati (ransomware)
- Cancellazione accidentale o dolosa dei dati da parte degli autorizzati
- Malfunzionamenti critici di hardware e software
- Disastri naturali

Quali sono le fonti di rischio?

- Fonti non umane - malfunzionamenti tecnici che causino la distruzione dei dati
- Fonti non umane - disastri (incendi, alluvioni, ecc.) che causino la distruzione dei supporti di memoria ove sono conservati i dati
- Fonti umane esterne - criminali informatici
- Fonti umane interne - amministratori di sistema, designati, responsabili o autorizzati negligenti
- Fonti umane interne - amministratori di sistema, designati, responsabili o autorizzati infedeli

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

- Formazione
- Tracciabilità
- Archiviazione
- Lotta contro il malware
- Manutenzione
- Controllo degli accessi logici
- Sicurezza dell'hardware
- Controllo degli accessi fisici

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

Importante.
In casi estremi di distruzione delle registrazioni (colposa o dolosa) gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.
Il rischio peggiore riguarda le ipotesi in cui le immagini rese indisponibili non possano essere utilizzate come prova a favore dell'interessato o a carico di terzi.

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

Limitata.
In generale, la minaccia relativamente più probabile risulta un'infezione ransomware che renda inaccessibili i dati. A seguire, in ordine, le minacce di malfunzionamenti critici di hardware e software utilizzati dal sistema, disastri naturali, comportamenti colposi degli autorizzati e infine la cancellazione dolosa di dati da parte di soggetti interni o esterni al Comune.
La probabilità di tali eventi è comunque contenuta date le misure di sicurezza tecniche e organizzative implementate dal Titolare.

Tuttavia, con riferimento specifico alle dashcam, il livello di rischio è aumentato dalla carenza di sistemi di controllo degli accessi. Le dashcam e le relative schede di memoria sono comunque custodite all'interno delle automobili della polizia locale, ciò che implica un controllo dell'accesso fisico ai dispositivi.

Inoltre, con riferimento alle dashcam e alle fototrappole, il rischio di perdita dei dati è incrementato dall'assenza di sistemi tecnici o di procedure idonee ad assicurare che i dati siano conservati per un periodo determinato.

Valutazione : Da correggere

Si rinvia alle valutazioni formulate ai paragrafi precedenti.

Criticità riscontrate e proposte per azioni correttive

Area tematica: Quali sono le risorse di supporto ai dati?

Valutazione: Da correggere
Con riferimento alle dashcam, il salvataggio di dati non crittografati e potenzialmente accessibili a chiunque abbia accesso fisico alle telecamere e strumenti idonei per collegarsi alle stesse comporta un rischio di perdita di riservatezza, integrità e disponibilità dei dati. Occorre introdurre un sistema che limiti la possibilità di accesso, modifica e cancellazione dei dati ai soli soggetti dotati di apposite credenziali.

Inoltre, la mancata definizione di procedure per il periodico controllo/salvataggio/cancellazione delle immagini comporta un rischio per la disponibilità dei dati, che potrebbero essere cancellati prematuramente ove le registrazioni siano mantenute attive per periodi più lunghi del previsto. Occorre introdurre un sistema che consenta di determinare con sicurezza il tempo di conservazione del dato.

I server di videosorveglianza collocati nei comuni dell'Unione non sono posizionati e gestiti nel rispetto di idonee policy di sicurezza fisica: occorre posizionare tutti i server in luoghi sicuri.

Area tematica: Qual è il periodo di conservazione dei dati?

Valutazione: Da correggere
Con riferimento alle dashcam, l'attivazione delle registrazioni non va lasciata all'iniziativa dei singoli agenti ma dovrebbe essere disciplinata da un apposito regolamento o mediante istruzioni impartite dal Titolare.
Con riferimento alle dashcam, la cancellazione dei dati tramite sovrascrittura non risulta sufficiente perché dipende dal loro effettivo utilizzo, e potrebbe quindi portare a una conservazione eccessivamente prolungata; occorre introdurre procedure per assicurare che i dati siano in ogni caso cancellati a scadenze determinate (ogni 7 giorni).
Con riferimento alle fototrappole, occorre introdurre procedure per assicurare che i dati siano in ogni caso cancellati a scadenze determinate (ogni 7 giorni).
Con riferimento al sistema di lettura targhe, il periodo di conservazione dei metadati (un anno) risulta sproporzionato rispetto alle finalità del trattamento, e andrebbe ridotto.

Area tematica: Misure a tutela dei diritti degli interessati

Valutazione: Da correggere
Con riferimento alle dashcam, occorre fornire un'informativa breve agli interessati, ad esempio esponendola sulle auto di servizio che sono dotate dello strumento.
Con riferimento ai sistemi di videosorveglianza tradizionale, di lettura targhe e di rilevamento automatico della velocità, è opportuno verificare la completezza della cartellonistica esposta.
Con riferimento alle fototrappole, è opportuno formalizzare delle istruzioni agli operatori sul posizionamento dei cartelli volti a fornire l'informativa breve.

Area tematica: Misure di sicurezza

Crittografia
Valutazione: Migliorabile
Estendere l'impiego di crittografia, ove possibile, anche ai client che si interfacciano con i vari sistemi di videosorveglianza in modo che le informazioni estratte in locale non siano facilmente carpibili.
Formazione
Valutazione: Migliorabile
È opportuno definire un piano di formazione che includa iniziative periodiche di sensibilizzazione e miglioramento.
Tracciabilità
Valutazione: Migliorabile
Valutare la possibilità di aumentare la tracciatura delle azioni compiute dagli operatori sui vari sistemi di videosorveglianza.
Backup
Valutazione: Migliorabile
Valutare l'introduzione di un sistema di backup remoto per i dati critici.
Controllo degli accessi fisici
Valutazione: Migliorabile
Si rinvia al paragrafo "Quali sono le risorse di supporto ai dati?"

Area tematica: Rischi

Valutazione: Da correggere
Si rinvia alle valutazioni formulate ai paragrafi precedenti.

Validazione sulla DPIA

Nome del DPO/RPD

GRC Team S.r.l. (referente Dott. Mattia Cortinovis)

Parere del DPO/RPD

In termini generali, il trattamento risulta proporzionato rispetto alle finalità perseguite, e sono adottate adeguate misure di sicurezza.
Alcuni elementi potenzialmente critici (condivisione dei dati con forze di polizia giudiziaria senza una formalizzazione dei rispettivi ruoli e responsabilità) emersi durante la DPIA sono stati risolti sospendendo le relative attività di trattamento fino alla necessaria regolarizzazione.
Occorre comunque risolvere tempestivamente le ulteriori criticità specifiche individuate nella presente DPIA in relazione alle dashcam, alle fototrappole, al sistema di lettura targhe e al sistema di video sorveglianza.
Le osservazioni formulate in relazione a dashcam e fototrappole sono estendibili anche alle bodycam; pertanto occorrerà tenerne conto nella selezione degli strumenti tecnici e nella progettazione delle loro modalità di utilizzo.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Data la tipologia di trattamento e il numero degli interessati non risulta necessario né pratico chiedere il parere di questi ultimi.