Valutazione di Impatto o
Data Protection Impact Assessment
Impianto Video Sorveglianza

Comune di Pedrengo

01 ottobre 2025 Aggiornamento DPIA

Sommario

1 Premessa

Il regolamento europeo sul trattamento dei dati impone al titolare di attuare delle azioni per la protezione delle informazioni e per il rispetto dei diritti degli interessati. Quando nella gestione dei dati si possano verificare dei rischi elevati a causa del monitoraggio sistematico dei comportamenti degli interessati, o per il gran numero dei soggetti coinvolti nel trattamento o per la tipologia dei dati stessi, il titolare è tenuto a realizzare una valutazione di impatto.
Scopo della presente DPIA è quello di valutare il livello di rischio nel trattamento dei dati e, laddove si rilevasse necessario, implementare le necessarie contromisure al fine di mitigare e diminuire l'impatto al fine di renderlo accettabile.

Nel caso ciò non fosse attuabile, o le misure di sicurezza previste dalla presente DPIA non vengano attuate, se il rischio residuo di trattamento risulti elevato, è compito del titolare del trattamento consultare l'autorità di controllo prima di procedere al trattamento poiché, secondo il dettato "Il titolare, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del GDPR, o all'art 23 del D.Lgs. 51/2018 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, oppure presenta un rischio elevato per i diritti e le libertà degli interessati".

Inoltre, se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità', presenta un rischio elevato per i diritti e le libertà' delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali.

La DPIA è un processo dinamico e ricorsivo che ha l'obiettivo di verificare il livello di rischio e di attuazione dei diritti degli interessati derivanti dal trattamento dei dati e di identificare eventuali azioni per ridurre il rischio stesso.

2 Quando è necessaria la DPIA

Nel caso in cui una tipologia di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, o preveda un trattamento di dati sensibili o biometrici, o un controllo esteso che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, al Titolare competente una valutazione di impatto (DPIA), prima di effettuare il trattamento, ai sensi dell'art. 35 del GDPR o del art. 23 D. Lgs 51/2018.
La valutazione dell'impatto del trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme sulla protezione dei dati, un rischio contenuto nella gestione dei dati, ed il rispetto dei diritti degli interessati. Si tratta di un processo diverso dalla valutazione dei rischi sulla protezione dei dati, in quanto valuta aspetti complessivi nell'ottica della verifica della corretta gestione dei diritti e delle libertà dell'interessato.
Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere ad una singola valutazione anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia diversa per un trattamento già in essere per gestire la stessa tipologia di dati per le medesime finalità. Oppure, un singolo processo di DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso.

Ai fini della decisione di effettuare o meno la valutazione di impatto si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dall'Autorità di controllo ai sensi dell'art. 35, paragrafi 4-6, del GDPR.

1.1 La Data Protection Impact Assessment:

Il working party ex-art. 29 (wp248 del 4 aprile 2017 con modifiche adottate il 4 ottobre 2017) "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" richiama il Considerando 84 del Regolamento in quale indica che l'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta le norme sulla protezione dei dati. "In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati e dalla direttiva 2016/680, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Al contrario, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

Le linee guida riportano 9 criteri per favorire l'identificazione di trattamenti con un "rischio potenziale elevato", ritenendo necessaria la valutazione d'impatto in presenza di almeno 2 criteri individuati su uno specifico trattamento di seguito descritto.

Criteri	
1)Valutazione o assegnazione di un punteggio	**X**
2) Processo decisionale automatizzato	**X**
3) Monitoraggio sistematico	**X**
4) Dati sensibili o aventi carattere altamente personale	**X**
5) Trattamento su larga scala	**X**
6) Creazione di corrispondenze o combinazione di insiemi di dati	**X**
7) Dati relativi a interessati vulnerabili	**X**
8) Uso innovativo di nuove soluzioni tecnologiche	**X**
9) impedimento all'esercizio di un diritto o di avvalersi di un servizio	**X**

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di eventuali codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli asset coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei ecc.).
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo di conservazione in funzione delle finalità o della normativa di legge;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- delle azioni di trattamento attuate dai responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati.

c) valutazione dei rischi sul trattamento di dati e sulla corretta attuazione dei diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono considerati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il Reg UE 2016/679 e D.Lgs. 51-2018, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;
e) l'acquisizione del parere del Responsabile della protezione dei dati personali.

Se la valutazione di impatto porta ad una quantificazione del rischio alta deve essere fatta una consultazione preventiva nei confronti dell'Autorità Garante prima di procedere al trattamento. Nel caso di rischio accettabile si procede a gestire il processo di trattamento avendo l'accortezza di applicare le misure necessarie per la protezione dei dati. Il documento attraverso il quale viene formalizzata la valutazione di impatto deve essere sottoscritto ed approvato dal titolare.

3 Obiettivo del documento

Il presente documento ha l'obiettivo di descrivere il processo metodologico con cui viene effettuata la DPIA dal Comune di Pedrengo, rappresentare i risultati della stessa in relazione ai trattamenti concernenti l'attivazione dell'impianto di video sorveglianza presente sul territorio dell'Ente.
Attraverso l'analisi verranno identificate le misure tecniche, organizzative e procedurali da adottare per un corretto trattamento dei dati e il contenimento dei livelli di rischi insiti nel processo di trattamento in seguito alle misure di protezione adottate. Nel caso in cui il risultato della valutazione di Impatto presenti un rischio elevato prima di attuare il trattamento deve essere fatta consultazione preventiva con l'autorità Garante della protezione dei dati.

Gli impianti di videosorveglianza installati o in corso di realizzazione dal Comune di Pedrengo, hanno come finalità principale la tutela della sicurezza urbana, della sicurezza pubblica, del patrimonio, della sicurezza stradale ed al supporto dell'attività di polizia amministrativa.

4 Normativa di riferimento

- **Regolamento UE n. 2016/679** 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;
- **Linee guida in materia di valutazione d'impatto** sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 adottate il 4 aprile 2017 (versione successivamente emendata e adottata il 4 ottobre 2017).
- **D.Lgs. 30 giugno 2003, n, 196,** recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- **D.Lgs. 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;
- **Decreto del Presidente della Repubblica n. 15 del 15.01.2018,** recante "Regolamento a norma dell'articolo 57 del D. Lgs 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";
- **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;

- **D.Lgs. 18/05/2018, n. 51 recante:** "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."
- circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/SICPART/421.2/70;
- **D.L. 23 febbraio 2009, n. 11**, recante: "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori ",
- **Provvedimento in materia di videosorveglianza**" emanato dal garante per la protezione dei dati personali in data 8 aprile 2010.
- **Linee guida n.3/2019** emanate dal Comitato europeo per la protezione dei dati (European Data Protection Board) sul trattamento dei dati personali attraverso dispositivi video).
- **Direttiva (UE) 2016/680** 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 Europeo.
- **D. Lgs 267/2000** Testo unico degli enti locali

Il Regolamento Europeo 2016/679 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" (cd "GDPR" o "Regolamento 679/2018 UE") è applicabile a partire dal 25 maggio 2018 e dispone che il titolare del trattamento di dati personali adotti tutte le misure necessarie al fine di garantire la sicurezza e la protezione dei dati.

La Direttiva 2016/680 del Parlamento europeo e del Consiglio d'Europa, 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, ha previsto e introdotto la regolamentazione delle protezione delle persone fisiche con riferimento al trattamento dei dati da parte delle autorità a fini di prevenzione, investigazione e repressione di reati.

In Italia, la direttiva 2016/680 è stata recepita con il D.Lgs. del 18 maggio 2018, n. 51 e tali norme hanno sostituito quelle presente nei titoli I e II della seconda parte del Codice Privacy, che erano dedicati al settore giudiziario e ai trattamenti dei dati da parte delle forze di polizia.

5 Documenti di Riferimento

I contenuti del presente documento traggono informazioni ed elementi di valutazione da:

- Regolamento per il Sistema di Videosorveglianza dell'ente adottato dal comune
- Procedure relative al data breach
- Atti di Nomina del Responsabile del commando di polizia locale e dei soggetti autorizzati

al trattamento delle immagini del sistema di video sorveglianza

- Atti di Nomina del Responsabile del trattamento dei dati per qui soggetti a cui il comune ha esternalizzato dei servizi quali quello della manutenzione dell'impianto di videosorveglianza
- Il Registro per le attività di trattamento dell'Ente;
- Le procedure e le policy adottate per la gestione della sicurezza dei dati

6 Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dato Personale Particolare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona."

Dati Giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3 comma 1, lettere da a) ad o) e da r) ad u) del DPR 14 novembre 2002, n 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati Membri

Responsabile: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (si tratta di un soggetto esterno all'organizzazione);

Designati ed Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Interessato: persona fisica, l'ente o l'associazione cui si riferiscono i dati personali.

SW: software

VPN: è una rete di telecomunicazioni privata, instaurata come connessione tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la suite di protocolli Internet.

archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico

Probabilità: valutazione della frequenza di accadimento di un evento, in funzione di eventi esterni non determinabili, delle vulnerabilità in essere e di eventuali contromisure implementate.

Impatto: indicazione del livello di incidenza di un evento che può compromettere la riservatezza, l'integrità e la disponibilità dei dati e dei diritti degli interessati;

Minaccia: evento potenziale, accidentale o deliberato, che, nel caso accadesse, produrrebbe un danno per l'interessato;

Vulnerabilità: debolezza intrinseca del sistema di gestione del dato che, qualora si realizzasse una minaccia, produrrebbe un danno all'interessato;

Rischio: è uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà. Il rischio in questa procedura è sempre riferito all'interessato

Contromisure: interventi tecnologici, procedure organizzative che possono essere implementate al fine di mitigare il Rischio Privacy associato ad ogni sistema o archivio e quindi diminuire il Rischio;

DPIA: data protection impact assessment

EDPB: European Data Protection Board (Comitato europeo per la protezione dei dati)

7 Campo di Applicazione

La presente analisi si applica al trattamento dei dati relativi all'impianto di video sorveglianza di contesto installato sul territorio del Comune di Pedrengo.

8 Compiti e responsabilità

Titolare dei trattamenti
La responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare ne monitora lo svolgimento consultandosi con il responsabile della protezione dei dati (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore.
Il Comune, in qualità di Titolare del trattamento, può impartire direttive e fornire indicazioni congiunte per la gestione ottimale della videosorveglianza;
Il Titolare adotta gli atti necessari per l'approvazione della DPIA.

Designato/Responsabile interno del Trattamento Dati: Per la videosorveglianza è il Comandante della Polizia Locale il quale partecipa alla valutazione di impatto e alla redazione della DPIA.
Supporta il titolare nell'adozione delle procedure di sicurezza ed organizzative per un corretto trattamento dei dati

Amministratore di sistema Informativo
Partecipa al processo di valutazione dei rischi e alla attuazione delle contromisure per il contenimento dei rischi.

Responsabile della protezione dei Dati
Unitamente al gruppo di lavoro supporta il Titolare nella valutazione di impatto relativa ad un particolare trattamento e ne sorveglia lo svolgimento in conformità alle prescrizioni normative.
Se richiesto esprime un parere sulla valutazione di impatto.

Componente del Team di Lavoro
La valutazione di impatto può richiedere la partecipazione di esperti dei processi di trattamento e della tecnologia utilizzata. Il soggetto in questione può essere sia persona interna all'organizzazione o esterna. Lo stesso è tenuto a fornire un apporto alla conduzione della DPIA nelle varie fasi.

9 Descrizione del contesto relativo al trattamento dei dati

9.1 Descrizione del Contesto

Il Comune di Pedrengo è dotato di un impianto di video sorveglianza composto da telecamere collegate tramite ponti radio, schede dati o rete cablata alla centrale operativa. I protocolli di comunicazione usano tecnologie sicure di trasmissione quali la cifratura.
Il sistema di video sorveglianza comprende dispositivi finalizzati a:

- acquisizione immagini videosorveglianza di contesto
- acquisizione immagini lettura targhe veicolari
- acquisizione immagini infrazioni semaforiche

L'attivazione dell'impianto di video sorveglianza ha lo scopo di migliorare l'efficacia dell'azione di protezione e tutela del patrimonio del Comune, di contrasto alla criminalità, agli illeciti amministrativi, di monitoraggio del territorio attraverso l'uso della tecnologia che consente di affiancare all'azione

del Titolare e del personale del Settore Polizia Locale un valido supporto sia preventivo che repressivo avvalorato dal contributo che questi strumenti offrono.

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. Le finalità del trattamento sono quindi determinate su tale base giuridica e necessaria per l'esecuzione di un compito svolto nel pubblico interesse e/o connesso all'esercizio di pubblici poteri.

Il posizionamento dei punti di ripresa sul territorio comunale è valutato dal Settore Polizia Locale sulla base delle criticità rilevate (es. episodi di criminalità, sinistri stradali, rilevazione di illeciti) che rendono opportuna e giustificata la presenza di postazioni di videosorveglianza. Parimenti, la verifica "storica" dell'utilizzo del sistema di videosorveglianza, sia per atti di iniziativa sia per richieste pervenute da FF.OO., conferma l'utilità per i fini in precedenza indicati di tutte le postazioni attualmente presenti, senza che siano individuabili postazioni di ripresa inutilizzate ovvero non motivate.

10 Attività di trattamento

DESCRIZIONE DELL'ATTIVITA' DI TRATTAMENTO	
Finalità di trattamento	Gestione impianto video sorveglianza per le seguenti finalità: ● attivare misure di tutela della pubblica sicurezza, la prevenzione, accertamento o repressione dei reati svolti sul territorio comunale; ● vigilare in materia di sicurezza urbana ● verificare la correttezza osservanza di ordinanze e/o regolamenti comunali per consentire l'accertamento dei relativi illeciti; ● rilevare le infrazioni al Codice della Strada, nelle modalità previste dalla Legge ● disporre di uno strumento operativo di protezione civile sul territorio comunale; ● essere d'ausilio nella ricostruzione dei sinistri stradali; ● monitorare la circolazione sulle strade; ● tutelare il patrimonio comunale e privato per la prevenzione e repressione di atti vandalici o di teppismo; ● prevenzione, accertamento e repressione degli illeciti derivanti dal mancato rispetto delle normative concernenti la gestione dei rifiuti; ● acquisire prove e filmati nell'ambito dell'attività di indagini di polizia giudiziaria; ● supporto all'attività di rispetto del codice della strada (es. verifica della copertura assicurativa e della revisione periodica dei veicoli).
Titolare del trattamento	Comune di Pedrengo
Contitolare del trattamento	-
Area che gestisce il trattamento	Comando Polizia Locale
Settore/ufficio	Sede Polizia – Comune di Pedrengo
Altri soggetti che accedono alla banca dati	Nessun soggetto esterno accede all'impianto in maniera autonoma
Incaricati al trattamento	Agenti di polizia locale incaricati
Responsabile dell'area designato al trattamento dei dati	Comandante del settore di Polizia locale
Soggetto terzo qualificato come responsabile del trattamento	Soggetto terzo che gestisce la manutenzione dell'impianto nominato responsabile del trattamento dei dati
Soggetto terzo qualificato come sub-responsabile del trattamento	Non Identificato
DPO	Identificato sul sito internet del comune

Descrizione del trattamento	
Finalità del trattamento	Gestione della Video sorveglianza di contesto
Base giuridica del trattamento	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 è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento nel caso i dati siano richiesti dall'autorità giudiziaria;
Tipologia di dati trattati	Dati personali, comportamenti illeciti soggetti a sanzioni amministrative, immagini di soggetti che compiono reati penali
Categorie degli interessati	Cittadini residenti e non residenti Proprietari dei veicoli
Perimetro in cui i dati sono trattati	Gli apparti di ripresa sono attivi h24 salvo il caso di guasti o attività di manutenzione
Modalità di trattamento	I dati vengono trattati in formato digitale, le telecamere che riprendono le immagini le trasmettono tramite connessione dati su rete privata o ponti radio che usano protocolli sicuri di comunicazione con il server installato nel comando di polizia locale
Tempi di conservazione dei dati	Immagini di contesto: i dati sono trattati per un periodo di 7 giorni e poi sono cancellati automaticamente dagli apparati di registrazione.
Destinatari a cui i dati sono comunicati	Autorità giudiziaria. Altre forze di polizia a fronte di una specifica e motivata richiesta o di un protocollo sottoscritto tra le parti. Altri soggetti nel rispetto della normativa di legge.
Diffusione dei dati	I dati non sono soggetti a diffusione
Valutazione della necessità e della proporzionalità del trattamento	
Necessità del trattamento.	Al fine di rendere efficace le attività identificate nelle finalità di trattamento il Comune di Pedrengo ha installato un impianto di video sorveglianza che è stato attivato in aree del territorio che hanno una importanza dal punto di vista della tutela della sicurezza o del monitoraggio del territorio quali ad esempio: ● Zone in cui sono presenti beni di proprietà dell'ente che potrebbero essere e sono stati oggetto di atti vandalici ● Parti della rete stradale di interesse per la circolazione ● Aree del territorio del comune che potrebbero essere oggetto di abbandono di rifiuti ● Zone del territorio che vengono monitorate per meglio tutelare la sicurezza dei cittadini quali luoghi pubblici e parchi pubblici per i quali sono state riscontrate attività che necessitavano di un controllo anche a fine preventivo
Proporzionalità del trattamento.	Il trattamento risulta proporzionato e non eccedente rispetto le relative finalità. La proporzionalità è stata applicata in ogni fase o modalità del trattamento, stabilendo: ● quando, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti; ● la dislocazione, l'angolo visuale, l'uso di zoom automatici e le tipologie - fisse o mobili - delle apparecchiature; ● la durata dell'eventuale conservazione (che, comunque, deve essere sempre temporanea).

	● nell'installazione delle telecamere è stata posta attenzione alle inquadrature e alla registrazione di spazi privati o aree sensibili (quali luoghi di culto, sedi di parti politici e sindacati istituti scolastici);
È stata effettuata una consultazione preventiva con gli interessati al trattamento	Il posizionamento degli impianti è stato proposto dal Settore Polizia Locale del comune e dal Titolare in relazione ad eventi accaduti nel corso del tempo e tiene conto delle esigenze degli interessati e del territorio di cui i cittadini non sono a conoscenza. L'impianto oggetto di analisi è stato in parte installato precedentemente all'entrata in vigore del GDPR. Il sistema ha subito una espansione, su questa porzione del sistema non è stata fatta una consultazione preventiva in quanto l'ente ha valutato la necessità di attuare misure: ● per la protezione del patrimonio, ● per il controllo del territorio ● e di attuazione delle misure di sicurezza urbana che tenga conto dell'incidenza di eventi sul territorio, delle strategie attuate dall'ente, dall'efficacia di questi strumenti a supporto dell'azione della polizia locale.
Asset usati per il trattamento	
Luoghi fisici	La sala di controllo è presso comando di polizia locale in un locale a cui accede solo il personale autorizzato. Le banche dati sono installate presso la sala server ospitata nella sede principale del comune
Hardware	Gli apparati di memorizzazione dei dati sono installati presso comando di polizia locale e sono dotati delle seguenti misure di protezione logica e fisica: ● Protezione tramite firewall ● Alimentazione con batterie di continuità ● Contratto di assistenza e manutenzione; ● Installazione su rete locale dedicata, separata dalla rete principale del Comune ● Accesso ai dati a soggetti autorizzati dotati di identificativo protetto da password
Apparati di ripresa	Gli apparati di ripresa sono installati sul territorio non conservano le immagini che vengono comunicate tramite rete geografica dedicata o ponti radio dedicati all'apparato di salvataggio delle riprese video.
Software	Il software di gestione delle registrazioni consente di ● Cifrare i dati registrare ● Creare diversi profili di accesso ai dati a seconda dell'incarico attribuito all'utente ● Registrare in file di log, le attività fatte dai diversi utenti
Reti di comunicazione	I sistemi di comunicazione dei dati tra apparati di ripresa e server di memorizzazione delle immagini usano protocolli sicuri di trasmissione
Possibilità accesso remoto	Accesso da remoto per interventi di manutenzione viene monitorato dal personale della Polizia Locale
Diritti degli interessati	
Come sono stati informati gli interessati	L'Interessato è informato in maniera chiara ed esaustiva in merito alle finalità del trattamento, alla durata di conservazione delle riprese, ai diritti che ha la facoltà di esercitare.

	Il comune ha predisposto dei cartelli informativi che segnalano le aree sottoposte a video sorveglianza. Il Titolare ha anche provveduto a predisporre una informativa di dettaglio pubblicata sul sito istituzionale. Nell'informativa sono indicate le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e i diritti dell'interessato secondo quanto previsto dal Reg UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e al D.Lgs. 51/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
Accesso ai dati da parte degli interessati	L'accesso ai dati è consentito nel caso in cui le immagini riprendono solo il soggetto interessato o in base alle disposizioni della normativa sull'accesso agli atti amministrativi o in relazione norma di legge per la tutela dei propri diritti.
Rettifica dei dati	Le immagini registrate non sono soggette a rettifica trattandosi di riprese del cotesto in cui sono posizionate le telecamere Preventivamente è stata fatta una verifica delle inquadrature delle telecamere distribuite sul territorio al fine di valutare che le stesse non riprendano contesti in cui sono riconoscibili gli interessati quali: ● Spazi privati (cortili, balconi finestre di edifici privati) ● Luoghi di culto o spazi antistanti gli stessi ● Sedi di partiti politici o sindacati
Cancellazione	I dati vengono cancellati automaticamente entro 7 giorni, tempi stabiliti dal regolamento di video sorveglianza e sono indicati nell'informativa relativa al trattamento dei dati
Portabilità	Diritto non previsto per il tipo di trattamento
Opposizione	Nel caso in cui un cittadino ritenga che l'impianto di video sorveglianza limiti la propria libertà può fare una segnalazione al comando di polizia o al DPO come specificato sull'informativa del trattamento dei dati Preventivamente è stata fatta una verifica delle inquadrature delle telecamere distribuite sul territorio al fine di valutare che le stesse non riprendessero contesti in cui sono riconoscibili gli interessati quali: ● Spazi privati (cortili, balconi di edifici privati) ● Luoghi di culto o spazi antistanti gli stessi ● Sedi di partiti politici o sindacati
Limitazione di trattamento	Il trattamento è stato attuato in sezioni del territorio in cui l'amministrazione ha ritenuto opportuno attivare l'impianto di video sorveglianza. I dati vengono trattati per un tempo limitato come indicato nell'informativa
Revoca del consenso	Il trattamento non si basa sul consenso al trattamento dei dati
Limitazione della finalità	I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità Il trattamento delle immagini relative all'impianto di video sorveglianza è fatto esclusivamente per le finalità dichiarate nel regolamento adottato dal Comune in materia di Video sorveglianza e specificato nell'informativa relativa al trattamento dei dati.

	L'accesso ai dati è regolamentato e consentito solo a personale autorizzato dal titolare e dal comandante della polizia locale Le finalità sono rese note all'interno del regolamento e nelle informative relative al trattamento dei dati
Limitazione della conservazione	I dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati I dati sono conservati su server installato nella sede del Comune Le registrazioni della video sorveglianza sono conservate per 7 giorni lavorativi al termine del quale il sw di gestione del sistema di video sorveglianza provvede a cancellare le immagini attraverso processo irreversibile.
Integrità e riservatezza	Il comune ha adottato opportune misure di sicurezza tecnologiche ed organizzative per la protezione dei dati quali Misure di protezione dell'edificio descritte nel piano di sicurezza informatica Accesso ai locali in cui sono presenti le banche dati (immagini) e i monitor di visualizzazione delle immagini al personale autorizzato Misure di protezione tecnologica quali • Accesso alle banche dati attraverso profili assegnati a personale autorizzato; • Registrazione in file di log non modificabile delle operazioni eseguite sulle immagini; • Protezione degli apparati di registrazione delle immagini con tool di sicurezza; • Formazione dei soggetti autorizzati ad accedere ai dati; • Separazione della rete di gestione delle immagini dalla rete dati del comune • Cifratura dei dati registrati sul server
Coinvolgimento del DPO	Il DPO nominato dall'ente è stato coinvolto nella realizzazione della DPIA

11 Privacy by design e by default

L'installazione o l'uso dei sistemi di video sorveglianza in aree pubbliche o soggette a pubblico passaggio, nell'ambito del territorio comunale è effettuata sulla base del legittimo interesse del titolare o in relazione dei fini istituzionali e dei poteri attribuiti allo stesso.
Il provvedimento dell'autorità Garante del 2010, richiamato da un più recente provvedimento del 22 Febbraio 2018 – afferma che "la rilevazione delle immagini può avvenire senza consenso, qualora, sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto possibili furti, danneggiamenti, o per finalità relative alla sicurezza del lavoro.
Il Comune di Pedrengo ha valutato che per rendere più efficacie l'azione del servizio di polizia locale al fine di promuovere la sicurezza urbana, e di tutelare i cittadini ed i beni pubblici, sia necessario avvalersi di impianti e tecnologie di video sorveglianza, poiché risultano non sufficientemente efficaci altri provvedimenti, tra i quali il costante impiego di operatori di Polizia a pattugliamento delle zone di interesse.
La progettazione e realizzazione dei sistemi di videosorveglianza prevede che gli impianti siano realizzati rispettando i principi previsti dalla normativa sulla protezione dei dati.

- Adeguamento ed applicazione del principio di proporzionalità e di minimizzazione nel

raccogliere e trattare i dati;
- Rispetto del principio di finalità del trattamento e della normativa che regolamentano i sistemi di video sorveglianza;
- Rispetto dei tempi di conservazione;
- Idonea ed adeguata informativa agli interessati di primo e/o secondo livello;
- Protezione dei dati registrati e conservati consentendo l'accesso agli stessi al solo personale autorizzato;
- Adeguati standard tecnologici tali da garantire le misure minime di protezione a tutela degli interessati;
- Protezione dei dati registrati consentendo l'accesso agli stessi al solo personale autorizzato;
- Istruzione e Formazione dei soggetti autorizzati al trattamento
- Applicazione delle "misure minime di sicurezza" previste dalla normativa e di adeguate misure di protezione in grado di garantire riservatezza, integrità e disponibilità;
- Analisi dei rischi eseguita ai fine di identificare eventuali criticità nel trattamento delle informazioni acquisiste mediante gli impianti e per la verifica del rispetto dei diritti degli interessati.

12 Valutazione dei Rischi Per Diritti E Libertà Degli Interessati

12.1 Premessa

Come previsto dal Reg UE 2016/679 e dalla Direttiva UE 2016/680 qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.
La valutazione del rischio nella DPIA ha l'obiettivo di verificare il rispetto dei diritti degli interessati.
Nell'ambito dell'applicazione del Regolamento, il rischio per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, sono da intendersi, quindi, come eventi che possono generare effetti negativi, o impatti, sugli Interessati, come un danno fisico, materiale o immateriale. Il Considerando 75 del Regolamento ci aiuta ad individuare le tipologie di rischi che possono derivare dal trattamento o dalla natura dei dati trattati, e che possono a loro volta essere classificati come:

Rischi per la sicurezza dei dati trattati, in termini di riservatezza, integrità e disponibilità, che possono comportare per gli Interessati, ad esempio, discriminazione, furto o usurpazione d'identità, danneggiamento dell'immagine e della dignità, pregiudizio alla reputazione, ecc. Dove la violazione delle dimensioni di sicurezza dei dati (RID) e degli strumenti utilizzati (ad esempio sistemi informatici o mezzi cartacei) possono essere la causa degli effetti negativi sugli interessati, è necessario identificare le minacce che potrebbero causare l'evento dannoso e portare ad accessi illegittimi, modifiche indesiderate e perdita dei dati (Linee Guida per la DPIA del Working Party article 29, n. wp248 rev1.0). Tali rischi possono essere ricondotti, pertanto, alla definizione più generale di "violazione dei dati personali", c.d. *data breach*, che, se non affrontata in modo adeguato e tempestivo, può provocare danni, materiali o immateriali alle persone fisiche.

Rischi che possono derivare da un trattamento non conforme ai principi generali del Regolamento e limitare i diritti e le libertà degli interessati, come ad esempio:
un trattamento di dati effettuato per finalità diverse rispetto a quelle dichiarate e legittime (principio di "limitazioni delle finalità");
un trattamento dei dati effettuato in assenza di una base giuridica legittima, come il fine istituzionale (principio di "liceità del trattamento");
un trattamento di dati eccedente rispetto alle finalità perseguite (principio di "minimizzazione dei dati");
un trattamento di dati non esatti o aggiornati (principio di "esattezza");
una conservazione dei dati, o la non cancellazione in base alle prescrizioni normative, per un periodo superiore a quello consentito per il conseguimento delle finalità legittime (principio di "limitazione della conservazione").

Rischi che possono impedire agli Interessati l'esercizio dei loro diritti ed il controllo sui dati personali che li riguardano, come ad esempio:
informazioni fornite agli Interessati non complete o chiare circa i termini del trattamento di dati personali che li riguardano (articoli 12, 13 e 14 del Reg UE 679/2016 e art 9 e 10 del Dlgs 51/2018)
Modalità e meccanismi non in grado di consentire la rettifica, la cancellazione, l'opposizione e la limitazione del trattamento da parte dell'Interessato (articoli da 16 a 19 e 21 del Reg UE 679/2016 o da 11 a 14 del Dlgs 51/2018);
Impossibilità per l'Interessato di esprimere la propria opinione o contestare una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona (articoli da 22 del Regolamento).

12.2 Analisi dei rischi

La valutazione del rischio è il processo complessivo di: identificazione del rischio, analisi del rischio e accertamento (in senso stretto) del rischio. I rischi possono essere valutati a livello di organizzazione, di dipartimento, per singoli trattamenti, per processi o attività individuali o per rischi specifici.
La valutazione del rischio fornisce una comprensione delle loro cause, delle conseguenze e connesse probabilità. Ciò costituisce l'input a decisioni del tipo:

- se l'attività di trattamento deve essere intrapresa, o no
- se i rischi devono essere trattati - scegliere tra opzioni con rischi differenti
- definire le priorità le opzioni di trattamento dei rischi (riduzione, trasferimento, accettazione e monitoraggio).
- selezionare le strategie più appropriate per il trattamento degli stessi, che possono condurre ad un livello tollerabile.

Per fornire una misurazione sul livello di rischio a cui l'organizzazione va incontro si utilizza un metodo **quantitativo** per valutare l'indice di rischio attraverso una valutazione legata a diversi parametri

Le definizioni applicate ai fini dell'analisi dei rischi sono:

- **Probabilità**: frequenza del verificarsi delle conseguenze;
- **Impatto**: qualunque conseguenza negativa derivante dal verificarsi dell'evento;
- **Indice Rischio (ID)**: combinazione della probabilità di accadimento di un danno e della gravità di quel danno. Per misurare il rischio l'ente utilizza la relazione:

IR: P x D in base alle seguenti scale:

Criteri per determinale la probabilità di accadimento		
P	Livello di probabilità	Criteri di valutazione
4	Alta	Accade di frequente
3	Media	Può accadere diverse volte
2	Bassa	Può accadere talvolta
1	trascurabile	Improbabile

Criteri per determinale l'Impatto		
P	Livello di impatto	Criteri di valutazione
4	Alta	Grave danno per i diritti e le libertà degli interessati
3	Media	danno Medio per i diritti e le libertà degli interessati
2	Bassa	danno Basso per i diritti e le libertà degli interessati
1	trascurabile	danno Trascurabile

12.2.1 Analisi Delle Minacce Applicabili

L'analisi delle minacce deve essere basata su un "insieme di minacce" derivanti da standard e best practices di riferimento, ognuna delle quali è caratterizzata da:

- uno o più scenari di rischio che la minaccia può determinare (accesso illegittimo ai dati, modifica non autorizzata dei dati, perdita dei dati, attacco informatico);
- la tipologia di asset sulla quale può agire;
- uno o più agenti di minaccia che possono attuarla (fonti umane interne/esterne o fonti non umane). Tra queste minacce occorre identificare quelle applicabili allo specifico

trattamento in esame.

12.2.2 Valutazione della Probabilità Di Accadimento Delle Minacce

Per ogni minaccia identificata come applicabile al trattamento in esame, occorre valutare la probabilità (P) di accadimento espressa su una scala di valutazione qualitativa discreta di 4 livelli (trascurabile, bassa, media, alta) prendendo in considerazione gli scenari di rischio per i diritti e le libertà degli interessati.
A tal fine, la probabilità viene derivata secondo un principio inversamente proporzionale al livello di efficienza delle misure predisposte per contrastarle e quindi dal livello di attuazione dei controlli posti in essere a protezione del trattamento relativamente ai seguenti ambiti:

- requisiti previsti dalle norme di legge e dai regolamenti applicabili;
- requisiti derivanti dalla normativa e dai pronunciamenti del Garante per la protezione dei dati personali;
- requisiti derivanti da standard e best practices internazionali di sicurezza e privacy
- adozione delle misure previsti nel regolamento di video sorveglianza e dalle procedure operative adottate dall'ente.

Nello specifico per ogni minaccia applicabile sono individuate le misure ritenute necessarie a contrastarla e per ogni misura l'insieme dei controlli che la costituiscono.

Ciò richiede che i controlli siano strutturati in "classi funzionali", ciascuna delle quali individua funzionalità omogenee di sicurezza e privacy in grado di contrastare le minacce applicabili, ovvero la misura che esse configurano. Ogni controllo inoltre deve essere caratterizzato da un livello di robustezza in merito alla modalità di attuazione:

- **Attuato**: il controllo è coperto da una o più contromisure pienamente e correttamente applicate;
- **Parzialmente attuato**: una o più contromisure coprono solo parzialmente il controllo espresso;
- **Non attuato**: il controllo non è coperto da alcuna contromisura oppure è solo parzialmente implementato;
- **N.A.:** il controllo non è applicabile al contesto di riferimento.

Il comune ha sviluppato questa attività di analisi die rischi ed ha sintetizzato il risultato di questo lavoro nella tabella successivamente riportata.
L'indice di rischio viene valutato attraverso il prodotto della probabilità di accadimento e del danno

Probabilità					
	IR	1	2	3	4
danno	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

	Rischio Trascurabile		Rischio Basso		Rischio Medio		Rischio Alto
	Monitorare		Monitorare		Azione Correttiva o piano di Miglioramento		Azione Correttiva

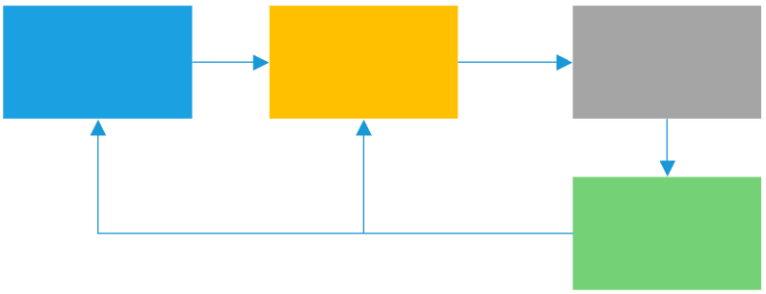
Nel caso in cui il rischio relativo ad un'attività di trattamento sia alto o altissimo si deve procedere con una mitigazione dello stesso adottando un'azione per il contenimento o la mitigazione e valutare l'esito di questa azione in termini di indice di rischio.

12.3 Modalità di trattamento del rischio

In seguito alle attività di analisi condotte occorre definire ed individuare la strategia di gestione del rischio per i diritti e le libertà degli interessati dell'ente.
Tale strategia scaturisce dalla identificazione degli asset tecnici, organizzativi e logistici che presentano criticità elevate e pertanto, controlli non adeguati a contrastare le eventuali minacce per il trattamento dei dati a cui essi sono rivolti. I piani di miglioramento o le contromisure da adottare vanno formalmente catalogati in documenti di analisi sulla base dei quali dovranno essere successivamente formulati i piani di miglioramento, quali parte integrante della documentazione a corredo della DPIA.
Le azioni vengono portate all'attenzione del Titolare che, valutato il livello di rischio effettivo, identifica quale tra le seguenti opzioni per il trattamento del rischio ritiene di adottare:

- evitare il rischio, rinunciando, ad esempio, alle attività che lo generano;
- condividere il rischio con un'altra parte in grado di gestire il rischio in modo più efficace, come ad esempio assicuratori e fornitori;
- ridurre il rischio ad un livello ritenuto accettabile, attraverso l'implementazione delle contromisure
- necessarie al raggiungimento di tale soglia;
- accettare il rischio se non si ritiene opportuna alcuna delle precedenti opzioni.

L'approccio sintetizzato nella seguente grafico:



Modalità di trattamento del rischio

Livello di rischio effettivo		Strategia di trattamento del rischio			
		Evitare	Condividere	Ridurre	Accettare
4	Alto	x	x	x	
3	Medio	x	x	x	
2	Basso			x	x

1	**Trascurabile**				x

Come si evince dalla tabella, la soglia di accettabilità del rischio è stabilita ad un livello di rischio basso o trascurabile, conseguentemente tutti gli altri casi, richiedono un trattamento al fine di ridurlo, trasferirlo o evitarlo. In ogni caso, anche quando il livello di rischio effettivo risulta limitato, l'ente deve valutare i costi di una eventuale riduzione, rispetto ai benefici per l'interessato e quindi valutare l'opportunità di ridurre tale rischio.
Se la strategia di trattamento approvata prevede la riduzione, occorre valutare il livello di rischio residuo che si raggiungerà a valle della applicazione della strategia scelta ed i requisiti da attuare per il suo conseguimento, che saranno successivamente dettagliati all'interno di specifici piani di sicurezza.

13 Valutazione di impatto

Nella tabella di seguito riportata sono riportati gli esiti della valutazione di impatto identificando in primis i controlli e le misure di sicurezza attuate

13.1 Misure di sicurezza organizzative attivate

Di seguito vengono descritte le misure di sicurezza adottate dall'ente per la tutela dei diritti degli interessati e la protezione dei dati.

13.1.1 Gestione Informativa

In tutte le aree in cui è stato attivato un sistema di video sorveglianza e prima di entrare nell'area di ripresa dei dispositivi installati è stata attivata una informativa come previsto dal Reg UE 2016/679 e dalla direttiva 680/2016 attraverso apposizione di cartellonistica che nel tempo verrà adeguata alle disposizioni delle linee guida 3/2019 dell'EDPB.
Il comune ha predisposto una informativa dettagliata pubblicata sul sito internet del comune

13.1.2 Durata del trattamento e periodo di conservazione dei dati

Come previsto dalle linee guida delle autorità garanti ed indicato nel Regolamento di videosorveglianza, il tempo di trattamento delle immagini tiene conto del principio di necessità, pertinenza e non eccedenza in ragione delle diverse tipologie di dati personali trattati e tenendo conto di ciascuna finalità in concreto perseguita. Il trattamento delle registrazioni degli impianti è conforme alla normativa di legge e ai provvedimenti dell'autorità Garante in attuazione alla normativa Europea e Reg UE 679/2016, Direttiva 680/2016 e nazionale D. Lgs 196-2003 e D Lgs 51-2018.
I sistemi di video sorveglianza installati sul territorio comunale prevedono una cancellazione automatica dei dati registrati nel rispetto della normativa.
In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di cancellazione dei dati registrati, la cancellazione delle immagini viene effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

i dati relativi alla videosorveglianza per la tutela della sicurezza urbana, ordine e sicurezza pubblica nonché di prevenzione o repressione dei reati oltre che di tutela del patrimonio, sono conservati per un congruo periodo e in particolare per tutto l'arco temporale nel rispetto dei diritti degli interessati tenendo di conto di successivi provvedimenti quali indagini o tempistiche inerenti all'esposizione di eventuali denunce/querele agli organi di polizia.
Nel caso in cui le registrazioni siano oggetto di successivo provvedimento i dati vengono conservati per il tempo necessario per la gestione del procedimento.

13.1.3 Regole adottate e principio di liceità in contesti particolari

Luoghi di Lavoro e relativi
Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature adibite a questa specifica finalità;
Non vengono quindi effettuate riprese al fine di controllare l'attività lavorativa quali ad esempio la produttività o il rispetto degli orari di lavoro. Nel caso di installazione di apparati di ripresa nei luoghi di lavoro la finalità degli stessi deve essere determinata dalla necessità di tutelare il patrimonio dell'organizzazione o per tutelare la sicurezza dei lavoratori. In tali casi, ai sensi dell´art. 4 della l. n. 300/1970, e della legge 183/2014 gli impianti e le apparecchiature, "dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo

accordo con le rappresentanze sindacali aziendali. In mancanza di queste, il datore di lavoro presenta istanza all'ispettorato del lavoro.
Tali garanzie sono state applicate dal comune sia nel caso di apparati installati all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad esempio, nel caso di telecamere installate su veicoli della polizia locale o all'interno dell'isola ecologica.

Istituti Scolastici
La presenza ed installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire "il diritto dello studente alla riservatezza" (art. 2, comma 2, d.P.R. n. 249/1998), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione.

In tali contesti l'utilizzo degli impianti di videosorveglianza può essere ammissibile per la tutela del patrimonio dell'ente, ed attivando gli impianti negli orari di chiusura degli istituti al fine di evitare la ripresa degli alunni e del personale scolastico;

Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale è delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio.

Luoghi di culto e di sepoltura
L'installazione di sistemi di videosorveglianza presso chiese o altri luoghi di culto o di ritrovo di fedeli è stato realizzato assumendo particolari oggetto di cautele, in funzione dei rischi di un utilizzo discriminatorio delle immagini raccolte e del carattere sensibile delle informazioni relative all'appartenenza ad una determinata confessione religiosa.
Al fine di garantire il rispetto dei luoghi di sepoltura, l'installazione di sistemi di videosorveglianza è ammessa in questi contesti solo quando si intenda tutelarle dal concreto rischio di atti vandalici o furti.

Sedi di partiti politici o sindacati
L'installazione dei sistemi di video sorveglianza tiene conto della particolarità di tali luoghi.
Videocamere che riprendano sedi di partiti politici o sindacati non sono presenti o hanno un grado di risoluzione tale o una visuale che non consentono di identificare i soggetti che accedono a questi luoghi.

Conservazione delle immagini
Al fine di rispettare le indicazioni della norma e rispettare i principi di pertinenza e minimizzazione il comune ha attivato delle procedure che prevedono la cancellazione automatica delle registrazioni nei sistemi di video sorveglianza. Le registrazioni, salvo il caso di procedimenti amministrativi o giudiziari previsti dalla legislazione nazionale che identificano le immagini come elemento probante, sono cancellati in modo automatico ed irrecuperabile (o in modo manuale laddove non tecnicamente attuabile un sistema automatico) alla scadenza dei periodi previsti dal regolamento di video sorveglianza adottato dall'ente e dalla normativa o linee guida in materia id protezione dei dati.

13.2 misure di sicurezza tecnologiche

Misure sicurezza attuate per il trattamento dei dati della video sorveglianza	
Sede Comune nel quale vengono trattati i dati – Piazza Elena Frizzoni e Via Monte Grappa, n. 1/a	
Video sorveglianza	Sul un lato del perimetro dell'edificio
Allarme antintrusione	Non presente allarme volumetrico
Antincendio	Estintori, idranti, porte sicurezza
Accesso all'edificio descrivere	Accesso principale e accesso polizia locale porta vetro con struttura in alluminio
Distribuzione chiavi registrata	SI
Misure sicurezza sala Operativa	
Accesso al solo personale autorizzato tramite porta chiusa a chiave	
Sede del Comando protetta da allarme dell'edificio	
Tutte le apparecchiature, di "recording" (storage) o le postazioni operatore, sono installate in ambienti sicuri, presidiati durante l'orario di lavoro e protetti da misure di sicurezza fisica	
Misure sicurezza sala server	
Accesso al solo personale autorizzato tramite porta chiusa a chiave	
Estintori installati localmente	
Climatizzazione della sala server	
Tutte le apparecchiature, di "recording" (storage) o le postazioni operatore, sono installate in ambienti sicuri, presidiati durante l'orario di lavoro e protetti da misure di sicurezza fisica	
Misure sicurezza organizzative	
Nomina del Designato individuato (responsabile comando di Polizia Locale), da parte dei Titolare nella figura del sindaco pro tempore	
Nomina formale degli autorizzati da parte del comandante del servizio di Polizia Locale	
Approvazione di una linea guida relativa alla protezione dei dati e di procedure che garantiscono i diritti degli interessati nel rispetto dei principi definiti dal Reg UE 2016/679 e D Lgs 51/2018.	
Adozione di procedure interne, alle quali i designati e i soggetti autorizzati dovranno attenersi, di accesso ai dati e che assicurino le condizioni e le garanzie per l'esercizio di tali diritti da parte degli interessati, qualora ciò sia appropriato alla luce delle finalità previste dallo specifico trattamento, oltre a misure tecniche e organizzative previste intese a ridurre al minimo il trattamento dei dati personali conformemente ai principi di proporzionalità e di necessità e quindi in modo lecito, corretto e trasparente nei confronti dell'interessato	
I soggetti autorizzati al trattamento dei dati dei sistemi di video sorveglianza sono operatori di Polizia Locale con qualifiche di Polizia Giudiziaria e Ausiliari di Pubblica Sicurezza	
Gli utenti, agenti di Polizia Locale con qualifica di agente o ufficiale di Polizia Giudiziaria e in possesso di qualifica di Pubblica Sicurezza, accedono ai sistemi di video sorveglianza con diversi profili a funzionalità diversificate e dedicate in base ai privilegi loro attribuiti a seguito di nomina scritta e impostati sul sistema.	
È stato impostato sui vari client e server o DVR o altri apparati che permettano l'accesso e la visualizzazione dei dati il blocco schermo con tempo impostato e necessità di password per effettuare nuovamente l'accesso	
Tutti i preposti e/o amministratori, in caso di necessità di allontanamento dalla postazione di videosorveglianza, nel caso abbiano effettuato un precedente accesso al rispettivo sistema e/o siano visualizzate immagini, prima di allontanarsi procederanno preventivamente ad effettuare	

una disconnessione dal sistema in modo tale che nessun altro, se non autorizzato e dotato di proprie credenziali, possa avere accesso ai dati registrati e/o alla visione live delle telecamere
Gli apparati di visualizzazione (monitor, schermi ecc.) del sistema sono posizionati e/o orientati in modo tale che in caso di presenza di pubblico presso gli uffici della polizia locale non sia consentito ai cittadini la visualizzazione delle immagini
È stata fatta la Formazione dei soggetti autorizzati relativa all'utilizzo degli apparati e alle misure di sicurezza da adottare per la protezione dei dati sia per quanto riguarda le norme sulla privacy e dei provvedimenti specifici relativi alla videosorveglianza
Nel caso di in cui vi sia l'esigenza da parte delle forze dell'ordine di accedere agli impianti di videosorveglianza del comune lo stesso sarà regolamentato da un accordo o da una convenzione che nelle regole le modalità di accesso da parte di soggetti esterni a Comune
Misure sicurezza tecnologica server
Protezione delle postazioni di lavoro tramite tools di sicurezza ed antivirus
Protezione della rete tramite apparati perimetrali (firewall)
Protezione del server tramite tools di sicurezza
Server alimentati con batterie di continuità
Impianto elettrico a norma
Vengono fatte delle copie di sicurezza delle cartelle del server nel quale sono eventualmente conservate delle registrazioni da conservare oggetto di un provvedimento
Misure sicurezza tecnologica video sorveglianza
I soggetti autorizzati accedono al software di gestione della sala di controllo della video sorveglianza con l'utilizzo di rispettive credenziali personali "sicure".
Gli utenti, accedono all'impianto di video sorveglianza e alle banche dati conservate secondo funzionalità diversificate e dedicate, attribuite dal Comandante della Polizia Locale. La suddivisione dei permessi dovrà essere organizzata secondo la seguente struttura: ● Gruppo che consulta le immagini ● Gruppo gestione ed esportazione ● Gruppo amministrazione ● Utente amministratore: gli utenti di questo gruppo accedono a tutte le funzionalità della piattaforma ed oltre a quanto descritto in precedenza hanno anche la facoltà di accedere ai tool di configurazione della piattaforma e del servizio e si occupano esclusivamente della manutenzione ordinaria e/o straordinaria del sistema e/o riparazioni guasti
Registrazione in un file di log non modificabile degli accessi, degli orari e delle operazioni eseguite con il software di video sorveglianza I log degli accessi dovranno essere conservati per almeno 90 giorni; La cancellazione dei dati è interdetta anche agli amministratori di sistema
I dispositivi di videoripresa non sono dotati di memorizzazione interna in quanto in caso di furto non garantirebbero una adeguata sicurezza delle videoriprese memorizzate. In caso di necessità tecnica di utilizzo di sistemi di memorizzazione interna le informazioni contenute dovranno essere memorizzate in modo cifrato al fine di garantire la sicurezza delle informazioni;
Il servizio di manutenzione, eventualmente gestito anche attraverso connessioni remote, dovrà avvenire con collegamenti sicuri attraverso protocolli di cifratura e accessi con credenziali sicure e personali attribuite ad ogni tecnico abilitato
Registrazione delle immagini in modalità cifrata
Cartelle in cui vengono eventualmente conservate le registrazioni sono profilate, ed autorizzazioni di accesso ai soli incaricati
Cancellazione automatica delle immagini al termine del periodo di conservazione tramite procedure che garantiscono l'irreversibilità del processo.

Trasmissione dei dati dalle telecamere alla centrale operativa tramite rete privata o ponti radio che usano protocolli di cifratura dei dati
Rete della video sorveglianza separata dalla rete dati principale del comune
Accessi ad internet e/o interconnessioni con altre reti, per collegamenti remoti (assistenza/accessi), da e verso internet per esposizione di servizi "da e verso" eventuali altre LAN (solo quella Comunale) attraverso Firewall con l'attivazione di idonee regole di controllo del traffico a difesa di eventuali intrusioni abusive nel sistema,
Eventuali device per visualizzazioni o accessi da postazioni o dispositivi mobili o remote, laddove implementati, adottano collegamenti con accessi attraverso credenziali sicure, personali e univoche per ogni singolo operatore autorizzato con i dati che non devono transitare e/o permanere su "cloud o server" di terzi se non in forma criptata. I collegamenti da remoto dovranno avvenire per tramite di collegamenti VPN o HTTPS
Le telecamere dovranno avere credenziali sicure di accesso, con profili di amministratore e user diversificati, al fine di poterle programmare e/o effettuare la prevista manutenzione solo da personale addetto

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Non rispetto diritti degli interessati							
Rischio che gli interessati possano essere non adeguatamente informati sul trattamento dei loro dati	Reclami degli interessati. Violazione delle libertà degli interessati	2	1	2	L'ente ha adottato delle procedure di gestione dell'informativa di primo livello sul trattamento dei dati che prevede cartelli segnaletici in prossimità delle aree video sorvegliate L'ente ha predisposto una informativa dettagliata pubblicata sul sito internet dell'Ente		
Rischi che i dati possano essere utilizzati non rispettando i limiti delle finalità per cui sono raccolti	Perdita di dignità, violazione delle libertà per l'interessato	1	2	2	I dati vengono raccolti per finalità legittime. Le telecamere sono posizionate in modo da non inquadrare contesti privati o non pertinenti con le finalità del trattamento - minimizzazione Il tempo di conservazioni delle immagini rispetta le indicazioni del provvedimento in materia di video sorveglianza dell'autorità garante sul trattamento dei dati		
Trattamento die dati in eccesso e non rispetto del principio di minimizzazione	Reclami degli interessati. Violazione dei diritti e delle libertà degli interessati	2	2	4	Le telecamere sono posizionate in modo da non inquadrare contesti privati o non pertinenti con le finalità del trattamento - minimizzazione I dati vengono raccolti per finalità legittime. I dati del sistema di video sorveglianza vengono cancellati attraverso procedure software entro 7 gg dalla data di registrazione		
Rischi che i dati possano essere trattati non	Non corretto trattamento die dati,	1	2	2	Le cartelle in cui sono salvati i dati sono profilata in modo che gli utenti accedano solo a dati di propria competenza		

rispettando il principio di esattezza	violazioni dei diritti degli interessati				Gli apparati installati sono omologati ed utilizzati per le finalità previste dalla normativa		
Rischi di accesso non autorizzato ai dati	Perdita di dignità, violazione delle libertà per l'interessato	2	2	4	Protezione della rete con apparati di sicurezza perimetrale che implementano funzionalità di sicurezza evolute quali IPS, content filtering Server su cui vengono salvati i dati protetto da misure di sicurezza tecnologica L'accesso alle banche salvate sui server viene fatto solo da soggetti autorizzati tramite utente protetto da password Accesso agli apparati di video sorveglianza attraverso utente e password e regole di autenticazione Le credenziali di accesso ai dati vengono periodicamente cambiate Rete della video sorveglianza separata dalla rete principale del comune Le postazioni di lavoro e i server della video sorveglianza sono protetti con tool di sicurezza Le cartelle in cui sono salvati i dati sono profilata in modo che gli utenti accedano solo a dati di propria competenza		
Rischi che i dati siano conservati per un periodo superiore a quanto previsto dalla normativa di legge o alle finalità del trattamento	Violazione dei diritti dell'interessato - Violazione del principio dell'oblio Riservatezza Integrità	1	2	2	I dati del sistema di video sorveglianza vengono cancellati attraverso procedure software entro 7 gg dalla data di registrazione Il comune ha adottato delle direttive per l'utilizzo dell'impianto/tecnologia di video sorveglianza L'ente ha adottato le procedure previste dalla normativa sulla protezione dei dati per un corretto trattamento degli stessi Le immagini non sono soggette a diffusione		

					Il tempo di conservazioni delle immagini rispetta le indicazioni del provvedimento in materia di video sorveglianza dell'autorità garante sul trattamento dei dati		
					I dati relativi alla gestione dell'impianto non vengono trasferiti al di fuori dello spazio della U.E.		
Rischi che l'interessato possa avere difficoltà ad esercitare i suoi diritti (es. diritto alla cancellazione o modifica del dato) o che i suoi diritti vengano violati	Violazione dei diritti dell'interessato - Reclami degli interessati Sanzioni dell'autorità garante	1	2	2	I dati vengono raccolti per finalità legittime.		
					Il comune ha adottato delle direttive per l'utilizzo dell'impianto/tecnologia di video sorveglianza		
					L'ente ha adottato le procedure previste dalla normativa sulla protezione dei dati per un corretto trattamento degli stessi		
					Regole per l'accesso alle immagini da parte degli interessati è definito nel regolamento di video sorveglianza e dalle norme di legge		
					Le policy di accesso agli atti sono definite nell'informativa al trattamento		
					L'ente ha nominato il responsabile per la protezione dei dati a cui l'interessato può rivolgersi per fare valere i propri diritti		
Trattamento dei dati non conforme alla normativa di legge o alle linee guida dell'Autorità garante per la protezione dei dati.	Violazione dei diritti dell'interessato - Reclami degli interessati	2	2	4	I dati vengono raccolti per finalità legittime.		
					Le telecamere sono posizionate in modo da non inquadrare contesti privati o non pertinenti con le finalità del trattamento - minimizzazione		
					Il tempo di conservazioni delle immagini rispetta le indicazioni del provvedimento in materia di video sorveglianza dell'autorità garante sul trattamento dei dati		
					I dati relativi alla gestione dell'impianto non vengono trasferiti al di fuori dello spazio della U.E.		
					Le immagini potranno essere comunicate alle forze dell'ordine.		

	Sanzioni dell'autorità garante				I dati sono accessibili agli interessati attraverso procedure di accesso agli atti		
Rischi fisici							
Incendio	Violazione dei diritti dell'interessato - Reclami degli interessati- Disponibilità	1	2	2	Antincendio costituito da estintori manutenuti da ditta specializzata Presente impianto rilevazione incendi presso sede Comunale Antincendio costituito da estintori manutenuti da ditta specializzata Antincendio costituito da estintori manutenuti da ditta specializzata Impianto elettrico a norma, Periodicamente controllato		
Allagamento	Violazione dei diritti dell'interessato - Reclami degli interessati- Disponibilità	1	2	2	L'edificio del Comune è distante da corsi d'acqua e bacini idrici L'edificio della polizia Locale è distante da corsi d'acqua e bacini idrici Storicità dell'evento Bassa		
Distruzione di strumentazione da parte di persone malintenzionate	Violazione dei diritti dell'interessato - Reclami degli interessati- Disponibilità	1	2	2	Nella sede del comune è stato installato sistema di allarme che si attiva automaticamente Attivo impianto di video sorveglianza sul perimetro dell'edificio Comunale Nella sede della Polizia Locale è stato installato sistema di allarme che si attiva automaticamente Inferiate alle finestre dell'edificio della Polizia Locale Attivo servizio di Vigilanza Notturna sede Polizia Locale Attivo impianto di video sorveglianza sul perimetro dell'edificio della Polizia Locale		
Attacchi Fisici, Furti, Atti vandalici	Violazione dei diritti dell'interessato - Reclami degli	1	2	2	Nella sede del comune è stato installato sistema di allarme che si attiva automaticamente		

	interessati- Disponibilità- Disponibilità Integrità				Attivo impianto di video sorveglianza sul perimetro dell'edificio Comunale Nella sede della Polizia Locale è stato installato sistema di allarme che si attiva automaticamente Inferiate alle finestre dell'edificio della Polizia Locale Attivo servizio di Vigilanza Notturna sede Polizia Locale Attivo impianto di video sorveglianza sul perimetro dell'edificio della Polizia Locale		
Fenomeni climatici - eventi calamitosi (Uragani, Nevicate)	Violazione dei diritti dell'interessato - Reclami degli interessati - Disponibilità	1	2	2	Storicamente non si sono mai verificati eventi climatici/naturali particolarmente dannosi		
Terremoti	Violazione dei diritti dell'interessato - Reclami degli interessati - Disponibilità Integrità	1	2	2	Storicità dell'evento Bassa Edificio antisismico / Rischio sismico basso		
Furto degli apparati	Violazione dei diritti dell'interessato - Reclami degli interessati- Disponibilità Riservatezza	2	2	4	Nella sede del comune è stato installato sistema di allarme che si attiva automaticamente Attivo impianto di video sorveglianza sul perimetro dell'edificio Comunale Porta di accesso con chiusure di sicurezza Nella sede della Polizia Locale è stato installato sistema di allarme che si attiva automaticamente Inferiate alle finestre dell'edificio della Polizia Locale Attivo servizio di Vigilanza Notturna sede Polizia Locale		

	Integrità				Attivo impianto di video sorveglianza sul perimetro dell'edificio della Polizia Locale Porta di accesso con chiusure di sicurezza I locali nei quali sono installati gli apparati di registrazione delle immagini sono adeguatamente protetti Accesso ai locali in cui sono installati gli apparati della video sorveglianza tramite porta chiudibile a chiave I dispositivi sono installati in luoghi protetti e/o difficilmente accessibili; Nelle telecamere non permangono registrazioni di dati.		
Accesso non autorizzati a locali e/o in aree ad accesso ristretto	Violazione dei diritti dell'interessato - Reclami degli interessati- Disponibilità Riservatezza Integrità	2	1	2	Nella sede del comune è stato installato sistema di allarme che si attiva automaticamente Porta di accesso con chiusure di sicurezza I locali nei quali sono installati gli apparati di registrazione delle immagini sono adeguatamente protetti Accesso ai locali in cui sono installati gli apparati della video sorveglianza tramite porta chiudibile a chiave Locali del Comando sono presidiati durante orario di lavoro L'accesso alle banche salvate sui server viene fatto solo da soggetti autorizzati tramite utente protetto da password La registrazione delle immagini viene fatta in modalità cifrata		
Sicurezza delle Rete Trasmissione Dati e della Rete Informatica							
Rischi legati ad attacchi informatici	Violazione dei diritti dell'interessato - Violazione della dignità - Reclami degli interessati	2	2	4	L'ente ha adottato misure di sicurezza adeguate alla protezione dei dati (apparato di sicurezza perimetrale, software di protezione sugli apparati server e sulle postazioni di lavoro, rete della video sorveglianza separata dalla rete del comune ecc.)		

					Server su cui vengono salvati i dati protetto da misure di sicurezza tecnologica		
					L'accesso alle banche salvate sui server viene fatto solo da soggetti autorizzati tramite utente protetto da password		
					Accesso agli apparati di video sorveglianza attraverso utente e password e regole di autenticazione		
					Le credenziali di accesso ai dati vengono periodicamente cambiate		
	Riservatezza Disponibilità Integrità				La registrazione delle immagini viene fatta in modalità cifrata		
					La comunicazione dei dati tra apparati di ripresa e apparati di registrazione usa protocolli sicuri di comunicazione		
					Apparati di video sorveglianza protetti da misure di sicurezza tecnologica		
					Il software dio registrazione delle immagini registra in un file di log le attività fatte dagli utenti		
					Il software di video sorveglianza cancella in modo irreversibile le immagini dopo 7 giorni		
					Il software di gestione della video sorveglianza viene periodicamente aggiornato		
					Adozione di misure di sicurezza tecnologiche adeguate e protezione delle comunicazioni tramite protocolli sicuri		
Rischi legati all'accesso da parte di soggetti non autorizzati al trattamento dei dati	Violazione dei diritti dell'interessato - Violazione della dignità - Reclami degli interessati - Disponibilità Riservatezza Integrità	1	2	2	La registrazione delle immagini viene fatta in modalità cifrata		
					La comunicazione dei dati tra apparati di ripresa e apparati di registrazione usa protocolli sicuri di comunicazione		
					Apparati di video sorveglianza protetti da misure di sicurezza tecnologica		
					Il software dio registrazione delle immagini registra in un file di log le attività fatte dagli utenti		

					Il software di gestione della video sorveglianza viene periodicamente aggiornato		
					Adozione di misure di sicurezza tecnologiche adeguate e protezione delle comunicazioni tramite protocolli sicuri		
					Accesso agli apparati di video sorveglianza attraverso tool di controllo remoto che usano protocolli sicuri di trasmissione		
					L'ente ha sottoscritto un contratto di Assistenza con un fornitore specializzato e lo ha nominato responsabile del trattamento eterno		
Accesso non autorizzato ai locali per omessa sicurezza della struttura	Violazione dei diritti dell'interessato - Violazione della dignità - Reclami degli interessati - Disponibilità Riservatezza Integrità	1	2	2	Attivo impianto di video sorveglianza sul perimetro dell'edificio Comunale		
					Nella sede del comune è stato installato sistema di allarme che si attiva automaticamente		
					Porta di accesso con chiusure di sicurezza		
					I locali nei quali sono installati gli apparati di registrazione delle immagini sono adeguatamente protetti		
					Accesso alla sala di controllo consentita solo a personale autorizzato		
					Locali del Comando sono presidiati durante orario di lavoro		
					I dispositivi sono installati in luoghi protetti e/o difficilmente accessibili; Nelle telecamere non permangono registrazioni di dati.		
					L'ente ha adottato misure di sicurezza adeguate alla protezione dei dati		
					I soggetti esterni che devono fare attività di manutenzione si collegano con un tool di assistenza remota e vengono abilitati alla connessione da operatore di Polizia		
Mancanza di energia elettrica o instabilità della stessa	Disponibilità	1	1	1	Evento raro con conseguenze accettabili		
					I server sono alimentati da batterie di continuità		

Intercettazione delle informazioni trasmesse sulla rete informatica attraverso ponti radio	Riservatezza	1	2	2	La comunicazione dei dati tra apparati di ripresa e apparati di registrazione usa protocolli sicuri di comunicazione Rete della video sorveglianza separata dalla rete principale del comune		
Rischi legati ai Dati							
Modifica non autorizzata di dati	Violazione dei diritti dell'interessato Riservatezza Integrità	1	2	2	Protezione della rete con apparati di sicurezza perimetrale che implementano funzionalità di sicurezza evolute quali IPS, content filtering L'accesso alle banche salvate sui server viene fatto solo da soggetti autorizzati tramite utente protetto da password Accesso agli apparati di video sorveglianza attraverso utente e password e regole di autenticazione Le cartelle in cui sono salvati i dati sono profilata in modo che gli utenti accedano solo a dati di propria competenza Il software di gestione della video sorveglianza viene periodicamente aggiornato Rete della video sorveglianza separata dalla rete principale del comune		
Comunicazione illecita o non corretta delle immagini	Riservatezza - Diritti degli interessati	1	2	2	Le immagini potranno essere comunicate alle forze dell'ordine. Accesso alla sala di controllo consentita solo a personale autorizzato L'accesso alle banche salvate sui server viene fatto solo da soggetti autorizzati tramite utente protetto da password Accesso agli apparati di video sorveglianza attraverso utente e password e regole di autenticazione La registrazione delle immagini viene fatta in modalità cifrata		
		1	2	2	0		

Mancata eliminazione dei dati al termine del trattamento	Riservatezza - Diritti degli interessati				Il software di video sorveglianza cancella in modo irreversibile le immagini dopo 7 giorni L'ente ha adottato le procedure previste dalla normativa sulla protezione dei dati per un corretto trattamento degli stessi		
Trasferimento di dati all'estero	Riservatezza Mancato rispetto delle normative di legge	1	2	2	I dati relativi alla gestione dell'impianto non vengono trasferiti al di fuori dello spazio della U.E. L'ente ha adottato le procedure previste dalla normativa sulla protezione dei dati per un corretto trattamento degli stessi		
Danneggiamento delle banche dati dell'impianto di registrazione	Disponibilità	1	2	2	Il software di gestione della video sorveglianza viene periodicamente aggiornato L'ente ha sottoscritto un contratto di Assistenza con un fornitore specializzato e lo ha nominato responsabile del trattamento eterno Apparati di video sorveglianza protetti da misure di sicurezza tecnologica		
Rischi legati all'applicazioni software e agli apparati HW							
sottrazione/alterazione credenziali di autenticazione	Riservatezza Integrità	1	2	2	Le credenziali di accesso ai dati vengono periodicamente cambiate Protezione della rete con apparati di sicurezza perimetrale che implementano funzionalità di sicurezza evolute quali IPS, content filtering Server su cui vengono salvati i dati protetto da misure di sicurezza tecnologica		
Policy di backup non adeguate problemi nelle procedure di gestione delle copie di sicurezza	Disponibilità	1	2	2	La tipologia di trattamento non necessita che vengano fatte delle copie di sicurezza delle registrazioni		
Uso non autorizzato del software	Riservatezza	1	2	2	Le credenziali di accesso ai dati vengono periodicamente cambiate I dati sono adeguatamente protetti per il livello di rischio legato al furto o all'accesso non autorizzato		

Malfunzionamento degli apparati o del sw di gestione dei dati	Riservatezza Integrità	2	2	4	Rischio di malfunzionamento degli apparati accettabile L'ente ha sottoscritto un contratto di Assistenza con un fornitore specializzato e lo ha nominato responsabile del trattamento eterno		
Mancato aggiornamento del software o errori di funzionamento	Riservatezza Integrità	1	2	2	Il software di gestione viene periodicamente aggiornato Attivato contratto di manutenzione della piattaforma applicativa e degli apparati di ripresa		
Rischi legati ai soggetti autorizzati al trattamento							
Errori nel corretto trattamento dei dati da parte del titolare o da personale autorizzato	Disponibilità Riservatezza Integrità	1	2	2	I soggetti autorizzati ad accedere alle banche dati sono stati istruiti all'uso del sistema di video sorveglianza I soggetti autorizzati ad accedere hanno partecipato ad un corso di formazione in materia di protezione die dati		
Non consapevolezza nelle procedure di gestione	Disponibilità Riservatezza Integrità	1	2	2	I soggetti autorizzati ad accedere alle banche dati sono stati istruiti all'uso del sistema di video sorveglianza I soggetti autorizzati ad accedere hanno partecipato ad un corso di formazione in materia di protezione die dati Attivato contratto di manutenzione della piattaforma applicativa e degli apparati di ripresa		
Non applicazione delle corrette procedure di trattamento dei dati	Riservatezza	1	2	2	I soggetti autorizzati ad accedere alle banche dati sono stati istruiti all'uso del sistema di video sorveglianza I soggetti autorizzati ad accedere hanno partecipato ad un corso di formazione in materia di protezione die dati Il comune ha adottato delle direttive per l'utilizzo dell'impianto/tecnologia di video sorveglianza		

	Integrità				L'ente ha adottato le procedure previste dalla normativa sulla protezione dei dati per un corretto trattamento degli stessi		
Trattamento non corretto od illecito	Riservatezza	1	2	2	I dati vengono raccolti per finalità legittime. L'ente ha predisposto una informativa dettagliata pubblicata sul sito internet dell'Ente		
Diffusione illecita delle immagini	Riservatezza	1	2	2	Le immagini non sono soggette a diffusione		
comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Disponibilità Riservatezza Integrità	1	3	3	L'accesso alle banche salvate sui server viene fatto solo da soggetti autorizzati tramite utente protetto da password Accesso agli apparati di video sorveglianza attraverso utente e password e regole di autenticazione La registrazione delle immagini viene fatta in modalità cifrata Il clima di lavoro è positivo, non ci sono elementi che fanno pensare a problemi di questo tipo		

14 Conclusione Finale

In relazione alle finalità, alla natura del trattamento ed al contesto in cui è applicato, valutate le misure di sicurezza adottate, l'impianto oggetto di analisi non presenta particolari criticità in materia id protezione dei dati e rispetto dei diritti degli intenteresti per cui il Comune di Pedrengo non deve attuare azioni di mitigazione o gestione del rischio nel processo di trattamento.
Il Titolare, consultato e previa verifica da parte dello stesso Responsabile della Protezione dei Dati del presente documento, ritengono quindi che siano state attuate tutte le sufficienti e necessarie misure di sicurezza idonee ad attenuare i rischi e ricondurli a un livello accettabile.
Alla luce delle risultanze prodotte dalla presente DPIA, non si ritiene quindi necessario avviare una comunicazione preventiva all'Autorità Garante quale obbligo sussistente solo in assenza di misure di sicurezza idonee ad attenuare i rischi connessi al trattamento dei dati.

15 Allegati

Fanno parte della valutazione di impatto i documenti tecnici sui quali il report con elenco degli apparati e il report fotografico relativo alle inquadrature delle telecamere di contesto

16 Aggiornamento della Valutazione di Impatto sulla Protezione dei Dati (DPIA) per il Sistema di Videosorveglianza del Comune di Pedrengo: Integrazione del Progetto Esecutivo P@RVC 2.0

1. Premessa e Obiettivo dell'Aggiornamento

La Valutazione di Impatto sulla Protezione dei Dati (DPIA) originale, denominata DPIA-Pedrengo-VideoSorveglianzaContesto-rev01, è stata elaborata in data 27 dicembre 2023. Il suo scopo primario era analizzare e valutare il livello di rischio inerente al trattamento dei dati personali nell'ambito dell'impianto di videosorveglianza di contesto del Comune di Pedrengo. L'obiettivo era garantire la piena conformità al Regolamento Generale sulla Protezione dei Dati (GDPR) e al D.Lgs. 51/2018, attraverso l'identificazione e l'implementazione di contromisure atte a mitigare i potenziali impatti negativi sui diritti e le libertà degli interessati.

Al termine di tale valutazione, si era giunti alla conclusione che il sistema non presentava criticità elevate e che le misure di sicurezza adottate erano sufficienti a ricondurre i rischi a un livello accettabile, eliminando la necessità di una consultazione preventiva con l'Autorità Garante per la protezione dei dati personali.

Il presente documento si prefigge l'obiettivo di integrare le informazioni derivanti dal Progetto Esecutivo P@RVC 2.0, datato 28 gennaio 2025. Questo progetto descrive in dettaglio la realizzazione e l'implementazione di nuove postazioni P@RVC 2.0 specificamente dedicate alla rilevazione delle infrazioni semaforiche. L'aggiornamento della DPIA esistente con queste nuove specifiche tecniche e operative è fondamentale per mantenere un quadro completo e aggiornato del trattamento dei dati. L'analisi si concentrerà sull'impatto di tali modifiche sulla valutazione complessiva del rischio per i dati personali, con l'esplicito intento di confermare che il livello di rischio residuo permanga accettabile, in linea con la conclusione della DPIA originale, e che non emergano nuove condizioni che richiedano una consultazione preventiva con l'Autorità Garante.

La necessità di questo aggiornamento sottolinea la natura intrinsecamente dinamica e ricorsiva del processo di valutazione d'impatto. La DPIA stessa riconosce questo aspetto, affermando che è un processo continuo volto a verificare il livello di rischio e l'efficacia delle azioni per ridurlo. La differenza cronologica tra la data della DPIA iniziale e quella del Progetto Esecutivo rende questo aggiornamento non solo una formalità, ma un passo essenziale per assicurare la conformità continuativa e riflettere l'evoluzione tecnologica e operativa del sistema di videosorveglianza comunale. Questo approccio proattivo dimostra l'impegno del Comune di Pedrengo verso una gestione della protezione dei dati che si adatta ai cambiamenti e alle innovazioni.

2. Descrizione del Sistema P@RVC 2.0 e le Sue Funzionalità

Il sistema P@RVC 2.0 rappresenta una soluzione tecnologica avanzata e altamente specializzata, progettata per la rilevazione automatica delle infrazioni semaforiche, in conformità con l'Articolo 146 del Codice della Strada. Questo sistema si distingue dall'impianto di videosorveglianza di contesto più generico descritto nella DPIA originale per la sua finalità specifica e la sua architettura mirata.

Verranno installate due postazioni fisse P@RVC 2.0 sul territorio comunale:

- **Varco 1**: collocato in Viale Fratelli Kennedy, all'altezza dell'intersezione con Via del Caravaggio, in direzione Seriate
- **Varco 2**: posizionato sempre in Viale Fratelli Kennedy, all'intersezione con Via Pascoli, in direzione Scanzorosciate

La funzione primaria di queste postazioni è rilevare e fotografare i veicoli che commettono infrazioni semaforiche, fornendo il supporto necessario per la successiva verbalizzazione da parte della Polizia Locale, anche in assenza fisica degli agenti.

Componenti Hardware e Software Chiave

Il sistema P@RVC 2.0 è un'unità integrata che racchiude tutti gli elementi essenziali per il suo funzionamento. Il corpo telecamera P@RVC 2.0 incorpora:

- Una telecamera a colori da 2 Megapixel, destinata alla documentazione delle infrazioni tramite immagini e video, e all'analisi dello stato delle lanterne semaforiche
- Una telecamera in bianco e nero da 5 Megapixel con filtro IR, ottimizzata per l'analisi dei transiti e l'acquisizione OCR (Optical Character Recognition) delle targhe, con configurazioni che hanno superato le prove UNI10772:2016
- Un illuminatore IR per garantire un'illuminazione uniforme
- Un'unità di elaborazione e archiviazione dei transiti
- Un'unità GPS per la geolocalizzazione precisa
- Un modulo I/O per l'interfaccia con le fasi semaforiche

Un aspetto fondamentale per la protezione dei dati è che le immagini acquisite vengono firmate digitalmente, rendendole di fatto immodificabili, e possono essere criptate in un unico file protetto da password, decriptabile esclusivamente dal software centrale al momento dell'inserimento nel database. Questa misura rafforza significativamente l'integrità e la riservatezza delle prove raccolte.

A livello periferico, ogni postazione è dotata di un armadio esterno (modello GEWISS GW 46003 IP66 con doppia chiusura di sicurezza) che contiene gli apparati di alimentazione, un gruppo di continuità (UPS) con batteria, un modulo di diagnostica remota e un Router UMTS 4G (Robustel R3000-L4L) per la comunicazione. È importante notare che l'unità elettronica principale (elaboratore e fotocamera) del P@RVC 2.0 è contenuta all'interno della propria custodia, separata dall'armadio periferico. Questa architettura garantisce che un eventuale danneggiamento dell'armadio non comporti la perdita dei dati e delle immagini rilevate, fornendo un ulteriore strato di sicurezza fisica.

Il cuore del sistema centrale è il software SRI (Sistema Rilevamento Infrazioni), ospitato nel Media Data Center Azure Cloud di Project Automation. Questo software permette agli operatori autorizzati di supervisionare le operazioni, archiviare i dati e le immagini acquisite dalle unità periferiche,

configurare le postazioni, analizzare le informazioni e gestire la diagnostica del sistema. Il software SRI implementa un sistema di login personale con gestione dei ruoli, consentendo l'accesso differenziato alle funzionalità in base al gruppo di appartenenza dell'operatore. Un elemento cruciale per la trasparenza e la responsabilità è il "Log Operazioni", che registra dettagliatamente gli eventi di login/logout e tutte le attività di accertamento svolte dagli operatori, inclusi data, ora, matricola e operazione eseguita. Questi log sono fondamentali per ricostruire le attività sul sistema e per garantire la sicurezza operativa e l'audit trail.

Processo di Acquisizione, Gestione e Validazione dei Dati

Il processo di gestione dei dati è altamente automatizzato e controllato. Le postazioni periferiche P@RVC 2.0 inviano automaticamente i dati e le immagini delle presunte infrazioni al sistema centrale SRI. Il personale della Polizia Locale, accedendo al sistema tramite un collegamento VPN sicuro e credenziali riservate, può validare le infrazioni in qualsiasi momento, 24 ore su 24, decidendo quali procedere alla verbalizzazione. Questa procedura ottimizza i tempi di gestione e le risorse logistiche. Il sistema offre anche la possibilità di mascherare automaticamente i veicoli non coinvolti nell'infrazione e di "spostare" (posticipare o non considerare) i transiti non validi, ad esempio in caso di targa illeggibile o di passaggio di mezzi di soccorso o delle forze dell'ordine.

Integrazione delle Finalità del P@RVC 2.0 con Quelle Già Previste dalla DPIA

Le finalità del sistema P@RVC 2.0, incentrate sulla rilevazione delle infrazioni semaforiche, si integrano e specificano le finalità più ampie di "sicurezza stradale" e "supporto all'attività di polizia amministrativa" già delineate nella DPIA originale. Il trattamento dei dati è fondato sulla base giuridica della necessità per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento, come già stabilito nella DPIA.

L'introduzione del sistema P@RVC 2.0 rappresenta un'evoluzione tecnologica significativa rispetto all'impianto di videosorveglianza di contesto generico. Le sue funzionalità specifiche, come la rilevazione semaforica, l'OCR delle targhe e la capacità di acquisire video dettagliati, unitamente alle misure di sicurezza integrate "by design" (firma digitale e cifratura delle immagini alla fonte, archiviazione protetta), dimostrano un approccio proattivo alla protezione dei dati. Queste misure vanno oltre le garanzie generiche inizialmente previste e rafforzano la base per una valutazione positiva del rischio, evidenziando un impegno concreto verso la protezione dei dati fin dalla fase di progettazione del sistema.

3. Aggiornamento delle Misure di Sicurezza Tecnologiche e Organizzative

L'integrazione del sistema P@RVC 2.0 introduce e rafforza diverse misure di sicurezza tecnologiche e organizzative, contribuendo a mantenere un elevato standard di protezione dei dati personali e a mitigare i rischi associati al trattamento.

Sicurezza della Trasmissione e Archiviazione dei Dati

La comunicazione dei dati tra le postazioni periferiche P@RVC 2.0 e il sistema centrale SRI avviene tramite una linea di comunicazione dedicata basata su tecnologia UMTS (4G). Questa trasmissione è protetta da un robusto meccanismo di cifratura: viene implementata una "VPN IPSEC in TUNNEL MODE". Questa configurazione cifra l'intero pacchetto IP e si basa su una "pre-shared key" nota solo ai due endpoint (il livello periferico e il livello centrale), assicurando che i dati in transito siano inintelligibili a terzi e che solo i peer autorizzati possano stabilire la connessione. Questo protocollo di sicurezza garantisce la riservatezza e l'integrità delle informazioni durante il trasferimento.

L'archiviazione centrale dei dati avviene presso il Media Data Center Azure Cloud di Project Automation. Questo Data Center è un punto di forza significativo, essendo certificato ISO/IEC 27001:2005 per la "Sicurezza delle informazioni dei servizi di noleggio sistemi di rilevamento infrazioni". L'utilizzo della piattaforma Microsoft Azure, riconosciuta per i suoi elevati standard di sicurezza, garantisce alti livelli di disponibilità, integrità e riservatezza dei dati.

L'accesso ai dati nel sistema SRI è strettamente controllato. Avviene tramite un'interfaccia web, ma solo previa attivazione di una VPN con credenziali riservate. Ogni operatore accede con un login personale (username e password), e le funzionalità disponibili sono rigorosamente definite in base al gruppo di appartenenza (controllo accessi basato sui ruoli), implementando il principio del "need-to-know".

Un'ulteriore misura di sicurezza fondamentale riguarda le immagini acquisite: queste vengono firmate digitalmente, rendendole di fatto immodificabili, e possono essere criptate in un file protetto da password, decriptabile solo dal software centrale. Questa pratica rafforza l'integrità e la riservatezza delle prove digitali, prevenendo alterazioni non autorizzate.

Misure di Minimizzazione e Proporzionalità

Il sistema P@RVC 2.0 contribuisce attivamente al principio di minimizzazione dei dati attraverso la sua capacità di mascherare automaticamente i veicoli non coinvolti nell'infrazione. Questo riduce la quantità di dati non pertinenti che vengono conservati. La DPIA originale già stabiliva che le telecamere fossero posizionate e configurate per non inquadrare contesti privati o non pertinenti alle finalità del trattamento, e che la proporzionalità fosse applicata nella dislocazione, nell'angolo visuale e nell'uso dello zoom. Queste garanzie rimangono valide e sono ulteriormente supportate dalla specificità delle ottiche (25mm/35mm) e dal posizionamento dettagliato delle telecamere come descritto nel Progetto Esecutivo.

Accountability e Audit Trail

Il software SRI integra un robusto sistema di "Log Operazioni". Questo registro dettagliato include tutti gli eventi di login e logout, nonché le attività di accertamento svolte dagli operatori, con indicazioni precise di data, ora, matricola dell'operatore e operazione eseguita. La DPIA originale

menzionava già la registrazione in file di log non modificabile delle operazioni, e il Progetto Esecutivo ne conferma e specifica la robustezza e la valenza. Questi log sono di importanza critica per ricostruire le attività sul sistema e per garantire la sicurezza di esercizio e la responsabilità individuale (accountability). La loro conservazione per almeno 90 giorni, come previsto, fornisce un solido strumento di audit e di verifica della conformità.

L'adozione di una certificazione ISO 27001 per il Media Data Center di Project Automation e l'utilizzo della piattaforma Microsoft Azure non solo attestano un elevato standard di sicurezza delle informazioni, ma implicano anche un trasferimento di parte della responsabilità operativa della sicurezza a entità specializzate. Questo approccio, pur offrendo benefici in termini di competenze e risorse dedicate, richiede che il Comune di Pedrengo, in qualità di Titolare del trattamento, si assicuri che i contratti con Project Automation (e, indirettamente, con Microsoft Azure) includano clausole di protezione dei dati conformi al GDPR (Data Processing Agreements - DPA). Tali accordi devono specificare chiaramente le misure di sicurezza adottate, i diritti di audit e la gestione dei sub-responsabili, garantendo la continuità della catena di responsabilità. Questo assicura che la strategia di "condivisione del rischio", come definita nella metodologia di trattamento del rischio della DPIA, sia formalmente e legalmente compliant.

4. Analisi e Riconciliazione del Periodo di Conservazione dei Dati

Uno degli aspetti più significativi emersi dall'integrazione del Progetto Esecutivo nella DPIA riguarda il periodo di conservazione dei dati, che presenta una discrepanza rispetto a quanto originariamente stabilito.

Identificazione e Analisi della Discrepanza

La DPIA originale indicava che i dati di videosorveglianza sarebbero stati trattati per un periodo di 7 giorni e successivamente cancellati automaticamente. Al contrario, il Progetto Esecutivo specifica che i dati nel server di sistema saranno conservati per un periodo massimo di sei mesi. Questa estensione del periodo di conservazione è una modifica sostanziale che richiede un'attenta giustificazione e un'analisi approfondita delle misure di mitigazione.

Giustificazione della Necessità di una Conservazione Più Lunga

La conservazione dei dati fino a sei mesi è strettamente necessaria per le specifiche finalità operative e legali del sistema P@RVC 2.0. Il sistema è progettato per la rilevazione delle infrazioni semaforiche al fine di "permettere la successiva redazione del verbale da parte della Polizia Locale" e per consentire la "validazione finale" delle infrazioni da parte del personale preposto. Questo processo implica la gestione di procedimenti amministrativi e legali (es. verifica delle infrazioni, accertamento, notifica delle sanzioni, gestione di ricorsi e contenziosi, supporto a indagini di polizia giudiziaria) che, per loro natura, richiedono tempi superiori ai 7 giorni. La DPIA originale aveva già previsto la possibilità di una conservazione più

estesa nel caso in cui le registrazioni fossero "oggetto di successivo provvedimento" o per "tempistiche inerenti all'esposizione di eventuali denunce/querele agli organi di polizia". Il sistema P@RVC 2.0, generando dati destinati a fini sanzionatori e probatori, rientra pienamente in questa casistica, rendendo la conservazione prolungata necessaria e proporzionata rispetto alle finalità perseguite.

Spiegazione Dettagliata delle Misure di Sicurezza che Mitigano il Rischio della Conservazione Estesa

Nonostante l'estensione del periodo di conservazione possa teoricamente aumentare il rischio di esposizione dei dati, il rischio residuo per i diritti e le libertà degli interessati è mantenuto a un livello accettabile grazie all'implementazione di robuste e specifiche misure di sicurezza tecnologiche e organizzative. Molte di queste misure sono dettagliate nel Progetto Esecutivo e rafforzano significativamente quelle già previste nella DPIA originale.

Le misure chiave che mitigano il rischio associato a una conservazione estesa includono:

Cifratura dei dati alla fonte e in archiviazione: Le immagini sono criptate già al momento della registrazione da parte delle telecamere P@RVC 2.0 e vengono conservate in formato cifrato sul server centrale. Questo rende i dati inaccessibili a soggetti non autorizzati anche in caso di accesso illecito all'infrastruttura di archiviazione.

Accesso strettamente controllato e basato sui ruoli: L'accesso ai dati è limitato esclusivamente al personale autorizzato della Polizia Locale. L'autenticazione avviene tramite credenziali personali e sicure, con profili di accesso diversificati (consultazione, gestione, amministrazione) che aderiscono rigorosamente al principio del "need-to-know", minimizzando l'esposizione non necessaria dei dati.

Log dettagliati e non modificabili: Il sistema SRI registra in un file di log non modificabile tutte le operazioni eseguite dagli utenti, inclusi accessi, orari e attività di accertamento. Questi log sono conservati per almeno 90 giorni e sono fondamentali per garantire la tracciabilità, l'accountability e per eventuali audit interni o esterni.

Certificazione ISO 27001 del Media Data Center: La centralizzazione del sistema presso il Media Data Center Azure Cloud di Project Automation, certificato ISO/IEC 27001:2005, attesta l'adozione di un sistema di gestione della sicurezza delle informazioni conforme agli standard internazionali. Questo riduce significativamente i rischi legati all'archiviazione dei dati in un ambiente cloud.

Trasmissione sicura dei dati: La comunicazione tra le unità periferiche e il server centrale avviene tramite una VPN IPsec in Tunnel Mode su rete UMTS 4G dedicata. Questa tecnologia assicura la riservatezza e l'integrità dei dati durante il transito, proteggendoli da intercettazioni o alterazioni.

Mascheratura automatica: La capacità del sistema P@RVC 2.0 di mascherare automaticamente i veicoli non coinvolti nell'infrazione contribuisce a ridurre la quantità di dati personali non pertinenti conservati, in linea con il principio di minimizzazione.

La gestione di questa discrepanza sulla retention è un punto focale di questo aggiornamento. La giustificazione si basa sulla "necessità" per finalità legali e amministrative, che è un principio cardine del GDPR. Le misure di sicurezza rafforzate non solo mitigano il rischio di una conservazione più lunga, ma elevano lo standard di protezione complessivo del sistema. Questo trasforma una potenziale criticità in una dimostrazione di robustezza e conformità, evidenziando una comprensione approfondita dei principi di proporzionalità e gestione del rischio.

Confronto Periodi di Conservazione Dati e Mitigazioni

La tabella seguente riassume la discrepanza nel periodo di conservazione dei dati e le misure specifiche adottate per mitigarne il rischio, garantendo che la valutazione complessiva rimanga accettabile.

Caratteristica	DPIA Originale	Progetto Esecutivo	Giustificazione/Necessità	Misure di Mitigazione
Periodo di Conservazione	7 giorni con cancellazione automatica. Possibilità di conservazione più lunga per "successivo provvedimento" o indagini	Fino a un massimo di sei mesi nel server di sistema	La conservazione estesa è necessaria per consentire la "validazione finale" delle infrazioni da parte della Polizia Locale e per gestire i processi amministrativi e legali (verbalizzazione, notifiche, ricorsi, indagini)	- Cifratura dei dati alla fonte - Accesso controllato con profili basati sui ruoli - Log dettagliati e non modificabili - Certificazione ISO 27001 del Data Center - Trasmissione sicura tramite VPN IPsec - Mascheratura automatica dei veicoli non coinvolti

Conferma delle Procedure di Cancellazione Irreversibile

Al termine del periodo di conservazione stabilito (massimo sei mesi), i dati verranno cancellati automaticamente e in modo irreversibile dal sistema, in linea con il principio di limitazione della conservazione e le procedure già previste dalla DPIA originale. Saranno inoltre fornite al Comune le modalità operative per l'esecuzione autonoma del download di tali dati prima della loro definitiva cancellazione, qualora necessario per specifiche esigenze procedurali o legali.

5. Valutazione Complessiva del Rischio Residuo e Conclusioni

L'integrazione delle informazioni provenienti dal Progetto Esecutivo nella DPIA esistente ha permesso di effettuare un'analisi approfondita delle nuove funzionalità e dell'architettura del sistema P@RVC 2.0 per la rilevazione delle infrazioni semaforiche. Sebbene l'introduzione di un sistema più specializzato, l'adozione di un ambiente di archiviazione cloud e l'estensione del periodo di conservazione dei dati rappresentino modifiche significative rispetto al contesto iniziale, l'analisi conferma che la valutazione complessiva del rischio per i diritti e le libertà degli interessati rimane a un livello accettabile.

Questo risultato è attribuibile all'implementazione di un insieme di misure di sicurezza tecnologiche e organizzative robuste e specifiche, molte delle quali sono dettagliate nel Progetto Esecutivo e vanno a rafforzare le garanzie già presenti nella DPIA originale. In particolare, la cifratura delle immagini alla fonte, la trasmissione sicura tramite VPN IPsec, l'archiviazione in un Data Center certificato ISO 27001, i rigorosi controlli di accesso basati sui ruoli, la funzionalità di mascheratura automatica e i sistemi di logging dettagliati e non modificabili contribuiscono a mitigare efficacemente i rischi associati all'aumento del volume e del periodo di conservazione dei dati.

La metodologia di valutazione del rischio adottata dalla DPIA classifica un rischio come "accettabile" se il suo Indice di Rischio (IR) rientra nella categoria "Basso" o "Trascurabile" (IR da 1 a 4), richiedendo in tal caso solo un'attività di monitoraggio. Le misure di contenimento del rischio adottate per il sistema P@RVC 2.0 assicurano che i rischi residui, anche quelli potenzialmente amplificati dalla maggiore specificità e dalla conservazione estesa dei dati, rientrino in questa soglia di accettabilità.

Pertanto, in linea con le risultanze della presente integrazione e con l'approvazione del Responsabile della Protezione dei Dati (RPD), si conferma che il Comune di Pedrengo ha attuato tutte le misure sufficienti e necessarie per attenuare i rischi e ricondurli a un livello accettabile. Di conseguenza, non si ritiene necessario avviare una consultazione preventiva con l'Autorità Garante, in quanto tale obbligo sussiste solo in assenza di misure di sicurezza idonee a mitigare i rischi connessi al trattamento dei dati. Il Comune continua a dimostrare un approccio proattivo e conforme alla normativa sulla protezione dei dati personali.

Bibliografia

- DPIA-Pedrengo-VideoSorveglianzaContesto-rev01 (27 dicembre 2023)
- Progetto Esecutivo P@RVC 2.0 (28 gennaio 2025)