COMUNE DI SERRAVALLE SCRIVIA
CORPO DI
POLIZIA LOCALE

IMPIANTO DI VIDEOSORVEGLIANZA

VALUTAZIONE D'IMPATTO
SULLA PROTEZIONE DEI
DATI PERSONALI

(ART. 35 Regolamento UE 2016/679)

TITOLARE DEL TRATTAMENTO: **COMUNE DI SERRAVALLE SCRIVIA**

AREA/SETTORE/SERVIZIO: **CORPO DI POLIZIA LOCALE**

DIRIGENTE/RESPONSABILE: Antonella Toscanini

DATA DEL DOCUMENTO: 30/06/2024

RESPONSABILE PROTEZIONE DATI (RPD): Avv. Massimo Ramello

Sommario

A. IN GENERALE

La Valutazione d'impatto sulla protezione dei dati rappresenta una delle principali novità introdotte dalla recente normativa in materia di protezione dei dati personali, in quanto correlata al principio generale di responsabilizzazione del Titolare del trattamento (accountability).

La Valutazione di impatto sulla protezione dei dati personali (nel seguito DPIA) è un processo che permette di valutare il livello di esposizione al rischio associato al trattamento dei dati personali e la necessità e proporzionalità del trattamento medesimo al fine di garantire e dimostrare la conformità dell'attività di trattamento con le prescrizioni normative.

A.1. Il RGPD

Il trattamento dei dati personali raccolti attraverso il sistema di videosorveglianza comporta l'applicabilità della normativa di protezione contenuta nel **REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016**, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati o RGPD).

L'**articolo 35 del RGPD** impone al Titolare di effettuare la DPIA prima di iniziare una data attività di trattamento che possa comportare "*un rischio elevato per i diritti e le libertà delle persone*", in particolare quando prevede di avviare un trattamento mediante "*utilizzo di nuove tecnologie, avuto riguardo alla natura, all'oggetto, al contesto e alle finalità del trattamento*".

L'**articolo 35 del RGPD** fa riferimento al possibile rischio elevato "*per i diritti e le libertà delle persone fisiche*". Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "*diritti e libertà*" degli interessati riguarda principalmente i diritti alla protezione dei dati ed alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

In linea generale il RGPD aiuta a comprendere come le casistiche di rischio possano avere probabilità e gravità diverse e derivare da attività di trattamento suscettibili di arrecare pregiudizi fisici, materiali o immateriali, in particolare se il trattamento possa comportare "*discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo*", la perdita di controllo da parte dell'interessato sui dati personali che li riguardano o privazioni o limitazioni nell'esercizio dei propri diritti fondamentali e libertà (v. **Considerando 75 del RGPD**).

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate avendo riguardo "*alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento*" (v. **Considerando 76 del RGPD**).

Dunque, occorrerà valutare se il trattamento riguardi "*dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza*" o sia finalizzato a valutare aspetti personali "*in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali*" o se si riferisca a "*dati personali di persone fisiche vulnerabili, in particolare minori*" o se riguardi "*una notevole quantità di dati personali e un vasto numero di interessati*" (v. **Considerando 75 del RGPD**).

Con riferimento ai trattamenti "*su larga scala*", ossia relativi ad una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potenzialmente presentano un rischio elevato, il RGPD incentra l'attenzione sulle categorie di dati particolari o sulle finalità delle attività di trattamento "*per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di*

categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza" (v. **Considerando 91 del RGPD**).

Infine, particolare attenzione deve essere posta su quei trattamenti che "*comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale*" (v. **Considerando 89 del RGPD**).

Il valore ed il ruolo della DPIA sono altresì chiariti nel **RGPD** all'interno del **Considerando n. 84** nei termini seguenti: "*Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di 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 redazione del documento di valutazione consiste, quindi, in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli).
Più nello specifico il documento illustra le considerazioni logiche che hanno accompagnato le fasi di identificazione, valutazione e risposta a tutti i rischi rilevati all'interno del trattamento oggetto di analisi.

Qualora l'esito della DPIA escluda la sussistenza di un rischio elevato, il Titolare può ritenersi legittimato ad eseguire il trattamento, in caso contrario, non potrà attivare il trattamento senza prima aver adottato le misure idonee a garantire un livello di sicurezza adeguato ai rischi per attenuarli o eliminarli.

Nell'ipotesi residuale in cui il Titolare non sia in grado di individuare dette misure tecniche od organizzative dovrà allora consultare l'Autorità di controllo, ai sensi dell'**articolo 36 del RGPD**, dando luogo alla c.d. consultazione preventiva.

Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (**articolo 35, paragrafi 1, 3 e 4 del RGPD**), lo svolgimento non corretto di una DPIA (**articolo 35, paragrafi 2, 7 e 9 del RGPD**) o la mancata consultazione dell'autorità di controllo competente ove ciò sia necessario (**articolo 36, paragrafo 3, lettera e) del RGPD** possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore alla citata soglia del 10 milioni di Euro.

A.2. Direttiva "POLIZIA"

Le peculiari finalità che caratterizzano il trattamento dei dati personali raccolti attraverso il sistema di videosorveglianza comportano l'applicabilità, altresì, 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, attuata in Italia con il **DECRETO LEGISLATIVO 18 maggio 2018, n. 51**.

L'**articolo 23 del D.Lgs. 51/2018** dispone che "*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 violazione delle disposizioni di cui agli **articoli 23 e 24 del D.Lgs. 51/2018**, in materia di DPIA, espone alla sanzione amministrativa del pagamento di una somma da 20.000 euro a 80.000 euro, salvo che il fatto costituisca reato.

Considerazioni analoghe a quelle (contenute nel RGPD) sopra riportate si ritrovano all'interno della Direttiva 2016/680 e, precisamente:

Considerando 51: *I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o dell'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; se sono trattati i dati genetici o biometrici per identificare in modo univoco una persona o se sono trattati i dati relativi alla salute o i dati relativi alla vita sessuale e all'orientamento sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi e la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; o se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*;

Considerando 52: *La probabilità e la gravità del rischio dovrebbero essere determinate con riferimento alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se il trattamento di dati comporta un rischio elevato. Un rischio elevato è un particolare rischio di pregiudizio dei diritti e delle libertà degli interessati*;

Considerando 58: *Nei casi in cui le operazioni di trattamento possano comportare un rischio elevato per i diritti e le libertà degli interessati in considerazione della loro natura, ambito di applicazione e finalità, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati, che verta in particolare sulle misure, sulle garanzie e sui meccanismi previsti per assicurare la protezione dei dati personali e per comprovare la conformità con la presente direttiva. Le valutazioni d'impatto dovrebbero riguardare i sistemi e processi delle operazioni di trattamento pertinenti, non singoli casi*;

Considerando 59: *Al fine di garantire un'efficace tutela dei diritti e delle libertà dell'interessato, il titolare del trattamento o il responsabile del trattamento dovrebbe consultare l'autorità di controllo, in determinati casi, prima del trattamento*;

Considerando 60: *Nella valutazione dei rischi per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati, come la distruzione, la perdita, la modifica accidentali o illecite o la divulgazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque trattati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. Il titolare del trattamento e il responsabile del trattamento dovrebbero provvedere affinché il trattamento dei dati personali non sia eseguito da persone non autorizzate*;

Considerando 61: *Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*.

A.3. Altre fonti normative

Disposizioni rilevanti in materia sono altresì contenute nei seguenti provvedimenti:

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI - 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 (di seguito: **Linee guida WP248**), adottate il 4 aprile 2017 e come modificate e adottate da ultimo il 4 ottobre 2017;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI - Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 (di seguito: **Linee guida WP250**), adottate il 3 ottobre 2017 ed emendate e adottate da ultimo in data 6 febbraio 2018;

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI PERSONALI (EDPB) - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, Versione 2.0, Adottate il 29 gennaio 2020

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI - Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 [**doc-web n. 9058979**].

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI - Provvedimento in materia di videosorveglianza - 8 aprile 2010 [**doc-web n. 1712680**]

A.4. Metodologia

I contenuti minimi della DPIA sono specificati come segue all'**articolo 35, paragrafo 7 del RGPD**:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

A norma dell'**articolo 23 del D.Lgs. 51/2018** "*La valutazione di cui al comma 1 contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente decreto*".

La metodologia qui adottata per la valutazione di impatto sulla protezione dei dati personali (DPIA), ai sensi dell'art. 35 RGPD, è sviluppata sulla base di quella definita da:
- **Commission nationale de l'informatique et des libertés o CNIL**, l'Autorità francese per la protezione dei dati, in conformità alle Linee guida WP248 e inclusa tra le metodologie raccomandate nell'allegato 1 delle Linee guida stesse;
- **Information Commissioner's Office o ICO**, l'Autorità inglese per la protezione dei dati personali;

Al fine di valutare i rischi e le modalità concretamente operative per la corretta protezione dei dati di terze parti, definiti 'interessati', si è proceduto alla valutazione dell'effettivo tipo di dati raccolti e trattati, del modo in cui detti dati vengono raccolti e trattati, dei metodi di conservazione custodia e protezione dei medesimi allo stato della valutazione, il tutto al fine di predisporre idoneo piano di

iniziative finalizzate all'adempimento degli obblighi dettati dal citato regolamento per la protezione dei dati, altresì noto come GDPR. Lo schema adottato è il seguente:
· la descrizione sistematica del trattamento e delle finalità;
· la descrizione della natura, dell'ambito, del contesto e degli scopi del trattamento;
· i dati personali trattati, i destinatari e il periodo per il quale sono conservati;
· una descrizione funzionale dell'operazione di trattamento;
· la descrizione dell'asset model su cui si basano i dati personali (es. Siti, hardware, software, reti, organizzazione, ecc.);
· la valutazione della necessità e la proporzionalità del trattamento;
· la descrizione delle misure previste per conformarsi al regolamento;
· la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degli interessati;
· la descrizione dell'origine, della natura, della particolarità e della gravità dei rischi;
· la determinazione delle misure previste per il trattamento di tali rischi;
· la descrizione del modo in cui sono coinvolte le parti interessate;
· il parere del Responsabile della Protezione dei Dati Personali (RPD);
· le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti

B. ANALISI PRELIMINARE DEL TRATTAMENTO OGGETTO DI VALUTAZIONE

L'analisi preliminare del trattamento è la prima fase del processo di valutazione del rischio ed è finalizzata a discriminare i trattamenti di dati personali che evidenziano un rischio elevato da quelli caratterizzati un rischio minore (di livello basso o medio). Essa serve quindi a **raccogliere le principali informazioni relative a uno specifico trattamento di dati personali** ed a decidere se esso debba essere sottoposto alla (sola) valutazione del rischio (in caso di rischio basso o medio per i diritti e le libertà delle persone fisiche) o alla DPIA (in caso di rischio elevato per i diritti e le libertà delle persone fisiche).

B.1. DESCRIZIONE SISTEMATICA DEL TRATTAMENTO
(art. 35, paragrafo 7, lettera a) del RGPD ed art. 23 del D.Lgs. 51/2018)

Indicazioni di **metodo**:
1. si tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento (**considerando 90 del RGPD**);
2. si dà una descrizione funzionale del trattamento;
3. sono indicati i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi;
4. si specificano gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
5. si tiene conto dell'osservanza di codici di condotta approvati (**art. 35, paragrafo 8, del RGPD**);

B.1.1 Il trattamento oggetto di analisi e valutazione è rappresentato da:

Un **sistema di videosorveglianza** costituito da dispositivi digitali nonché da software per acquisire immagini, gestirle e mostrarle ad un operatore. Sotto il profilo funzionale, I suoi componenti sono rappresentati da:
- i dispositivi di acquisizione delle immagini: servono a generare un'immagine del mondo reale in un formato tale da poter essere utilizzata dal resto del sistema;
- le interconnessioni: comprendono tutte le trasmissioni di dati all'interno dell'ambiente video, vale a dire, le connessioni (cavi, reti digitali e trasmissioni wireless) e le comunicazioni (segnali video e dati di controllo, digitali ed analogici);
- gestione delle immagini: analisi, estrazione, conservazione e presentazione;
- gestione del sistema: comprende la gestione dei comandi degli operatori e delle attività generate dal sistema (procedure di allarme, operatori di allarme);
- interfacce con altri sistemi: connessione con sistemi di sicurezza (ad es. controllo accessi, allarme antincendio) o non legati alla sicurezza (ad es. riconoscimento automatico delle targhe).

In particolare, il sistema di compone di:
a) Sistema di videosorveglianza con telecamere fisse di contesto posizionate ai varchi di accesso dell'area urbana e all'interno del concentrico, finalizzato al presidio del territorio stesso nonché alla vigilanza del traffico veicolare e pedonale;
b) Sistema di videosorveglianza con telecamere fisse per la lettura delle targhe posizionate nei varchi principali di accesso dell'area urbana con la funzione di video-analisi e ricerca della targa di un determinato veicolo anche all'interno di più impianti diversi;
c) Sistema di videosorveglianza con telecamere fisse posizionate presso il parco pubblico e gli istituti scolastici al fine di garantire la sicurezza urbana;
d) Sistema di videosorveglianza con telecamere fisse, posizionate per ragioni di sicurezza urbana e sicurezza stradale presso l'area interna ai binari della Stazione FF.SS. (con autorizzazione di R.F.I.) e lungo l'area comunale esterna e circostante la zona della Stazione Ferroviaria;
e) Sistema di videosorveglianza con telecamere fisse posizionate presso il cimitero e presso il magazzino comunale per ragioni di sicurezza urbana e sicurezza stradale;

f) Telecamere private con accesso riservato al Comando di Polizia locale e collegate al sistema di videosorveglianza cittadino;
g) Sistema di videosorveglianza mobile (fototrappole);
h) Body Cam (videocamere indossabili);
i) Sistema di lettura e riconoscimento automatico delle targhe dei veicoli (ALPR o ANPR)
La descrizione delle caratteristiche tecniche dell'impianto e dei suoi componenti è contenuta nella documentazione progettuale ed esecutiva allegata alla presente DPIA.

Di seguito sono evidenziate le **caratteristiche di maggior rilevanza sotto il profilo della protezione dei dati personali**.

B.1.2. Rilevanza territoriale

Trattandosi di un Ente territoriale, il sistema di videosorveglianza ha una **rilevanza limitata al territorio di competenza del Titolare**. Ai fini dell'applicabilità delle disposizioni contenute nel RGPD, il perimetro geografico di rilevanza è rappresentato da **persone fisiche che si trovino in Europa**.

B.1.3. Dati personali

Il progetto implica il trattamento di dati personali, nell'accezione contenuta all'**articolo 4 del GDPR paragrafo 1, n. 1 del RGPD**.

In particolare, il trattamento riguarda i dati personali raccolti attraverso gli strumenti di acquisizione video componenti il sistema.

L'identificazione delle persone fisiche non avviene in modalità automatica ma, bensì, a cura dell'operatore, il quale vi provvede sulla base delle informazioni così raccolte (conoscenza diretta) ed anche in combinazione con altri dati personali posseduti dall'Ente, ovvero acquisiti mediante procedimenti amministrativi di accertamento e verifica.

Di seguito sono elencate le categorie di dati personali oggetto di trattamento, distinte in ragione di quanto previsto dagli **articoli 6, 9 e 10 del RGPD** (al fine della verifica delle condizioni di liceità del trattamento).

CATEGORIE DI DATI PERSONALI TRATTATE

X	Informazioni grafiche o visive su tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici
X	Dati riguardanti la presenza ed il comportamento delle persone nello spazio considerato
N.A.	Registrazione audio
X	Coordinate GPS delle riprese (vedasi tabelle)
X	Data ed ora delle riprese
X	Modalità di svolgimento di fatti costituenti illecito amministrativo
X	Dati di immatricolazione dei veicoli
X	Dati relativi al transito dei veicoli
X	Dati idonei a consentire l'identificazione del soggetto responsabile della circolazione stradale
X	Modalità di svolgimento di fatti relativi ad un sinistro stradale
X	Modalità di svolgimento di fatti costituenti illecito penale

Categorie particolari di dati personali

In talune circostanze può verificarsi che il sistema di videosorveglianza determini il trattamento di dati c.d. "sensibili", nell'accezione di cui all'**articolo 9 del RGPD**. In particolare:

X	Dati personali che rivelino l'origine razziale o etnica
X	Dati personali che rivelino le opinioni politiche, le convinzioni religiose o filosofiche
X	Dati personali che rivelino l'appartenenza sindacale
N.A.	Dati genetici
N.A.	Dati biometrici intesi a identificare in modo univoco una persona fisica
X	Dati relativi alla salute
N.A.	Dati relativi alla salute vita sessuale
X	Dati relativi all'orientamento sessuale della persona

Le riprese video degli individui, raccolte dal sistema, non possono essere considerate dati biometrici ai sensi dell'**articolo 9 del RGPD** e dell'**articolo 7 del D.Lgs. 51/2018**, in quanto non sono sottoposte ad un trattamento tecnico specifico per contribuire all'identificazione di tale individuo (**articolo 4, paragrafo 1, n. 14, del RGPD e articolo 2, comma 1, lett. o) del D.Lgs. 51/2018**).

Dati giudiziari

Le particolari finalità che legittimano l'utilizzo del sistema di videosorveglianza rendono necessario il trattamento di dati personali relativi alla commissione di reati, nell'accezione di cui all'**articolo 10 del RGPD**. La raccolta riguarda unicamente le fattispecie potenzialmente costituenti reato, verificatesi nelle circostanze di tempo e di spazio oggetto di ripresa.

B.1.4. Operazioni (modalità) del trattamento

A norma dell'**articolo 4, paragrafo 1, n. 2 del RGPD**:
per "*trattamento*" s'intende "*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*".

Di seguito sono elencate le operazioni di trattamento, comunemente, attuate dal Titolare:

X	Raccolta
X	Registrazione
X	Organizzazione
N.A.	Strutturazione
X	Conservazione
X	Adattamento o modifica
X	Estrazione
X	Consultazione
X	Uso
X	Comunicazione mediante trasmissione
N.A.	Diffusione o qualsiasi altra forma di messa a disposizione
X	Raffronto
N.A.	Interconnessione
N.A.	Limitazione

X	Cancellazione
X	Distruzione
N.A.	Profilazione o scoring (Il riferimento è a meccanismi di profilazione o algoritmi predittivi che possano ad esempio impattare sulla situazione economica, sulla salute, sugli interessi personali, sul comportamento, sull'ubicazione, sugli spostamenti, sulle abitudini di consumo, sul rendimento professionale, ecc.)
N.A.	Adozione di decisioni automatizzate che possano produrre effetti giuridici per i destinatari, senza l'intervento di decisione umana
X	OCR - Riconoscimento ottico di caratteri presenti nelle targhe automobilistiche
X	Creazione e gestione di liste di veicoli transitati nelle aree soggette a ripresa
X	Monitoraggio in tempo reale presso il Comando

Particolare attenzione va posta in relazione a specifiche operazioni di trattamento, di seguito individuate:

I dati personali sono **raccolti**:

X	Osservando una zona accessibile al pubblico nella quale venga a trovarsi l'interessato
X	Presso banche dati pubbliche (PRA, Motorizzazione, ...)

Criteri di **conservazione** dei dati personali

X	7 giorni, in caso di non verificazione degli eventi presupposti dalle singole finalità del trattamento
X	Fino al passaggio in giudicato della sentenza che definisce il contenzioso nel quale sia necessario produrre le riprese video
X	Fino alla definizione del procedimento amministrativo nel quale siano utilizzate le riprese video

La **cancellazione** dei dati personali al termine del periodo di conservazione avviene

X	Con procedure automatizzate

I dati raccolti attraverso il sistema di videosorveglianza possono essere **comunicati**, nel rispetto delle norme di legge e regolamentari, a:

	accesso diretto in tempo reale	estrazione diretta dalla registrazione	estrazione su richiesta
Autorità giudiziaria			**X**
Forze dell'ordine	**X**	**X**	**X**
Altri soggetti pubblici			**X**
Privati			**X**
Interessato			**X**

Diffusione dei dati personali:

X	Non è prevista alcuna forma di diffusione delle immagini fotografiche e video raccolte dal sistema di videosorveglianza

L'utilizzo del sistema di videosorveglianza comporta il **trasferimento di dati all'estero**:

X	NO
X	SI, in ragione dell'utilizzo di servizi "Cloud", i dati sono trasferiti verso un paese europeo (body cam – fototrappola)
N.A.	SI, in ragione dell'utilizzo di servizi "Cloud", i dati sono trasferiti verso un paese terzo od un'organizzazione internazionale

B.1.5. Liceità del trattamento

Al fine di valutare la liceità del trattamento, occorre individuare dettagliatamente le finalità del trattamento (**articolo 5, paragrafo 1, lettera b) del RGPD**).

Le finalità del trattamento sono esplicite, specifiche e legittime. In particolare,
- sono **esplicite**: in quanto sono individuate all'interno del Regolamento approvato dall'Ente e sono indicate con chiarezza nelle informazioni rese all'interessato ai sensi degli **articoli 13 e 14 del RGPD**;
- sono **specifiche**: in quanto si riferiscono a tutte le componenti del sistema quali meglio dettagliate negli allegati alla presente valutazione;
- sono **legittime**: in quanto trovano adeguato fondamento nelle disposizioni contenute negli **articoli 6, 9 e 10 del RGPD**.

Il sistema di videosorveglianza è stato oggetto di regolamentazione ad opera del **Consiglio comunale, con la deliberazione n. 12 del 13.05.2021**
In data 27.02.2023 è stato sottoscritto il Patto per la Sicurezza Urbana tra il Sindaco ed il Prefetto.

Finalità del trattamento:
a) prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del D.L. 20 febbraio 2017 n. 14, convertito in legge, con modificazioni, dall'art. 1, comma 1, L. 18 aprile 2017, n. 48;
b) prevenzione, indagine, accertamento e perseguimento di reati od esecuzione di sanzioni penali;
c) prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado e abbandono di rifiuti, e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nel regolamento di polizia urbana, nei regolamenti locali in genere e nelle ordinanze sindacali, quando non risulti possibile, o si rilevi non efficace, il ricorso a strumenti e sistemi di controllo alternativi;
d) tutelare l'ordine, il decoro e la quiete pubblica;
e) controllare discariche di sostanze pericolose ed "eco-piazzole" per monitorare le modalità del loro uso, la tipologia dei rifiuti scaricati e l'orario di deposito;
f) dotarsi di uno strumento attivo di protezione civile, per la individuazione e la gestione delle aree e dei punti strategici, a fronte di emergenze;
g) monitorare il livello dei corsi d'acqua, in caso di eventuale superamento del livello di guardia, e monitorare situazione critiche causate da esondazioni od altri eventi calamitosi ai fini di protezione civile;
h) prevenzione e controllo degli incendi;
i) identificare luoghi e ragioni di ingorghi per consentire il pronto intervento della polizia locale;
l) rilevare le infrazioni al Codice della Strada, nel rispetto delle norme specifiche che regolano la materia;
m) ricostruire, ove possibile, la dinamica degli incidenti stradali;
n) identificare gli itinerari di afflusso e deflusso di veicoli o evacuazione dei cittadini, ai fini del piano di emergenza comunale;
o) rilevare le vie di maggiore intensità di traffico, i tempi di attesa dei servizi pubblici e quant'altro utile all'informazione sulla viabilità;
p) monitorare il traffico cittadino ed i relativi flussi, con dati anonimi, per un più razionale e pronto impiego delle risorse umane laddove se ne presenti la necessità, per la predisposizione di piani del traffico nonché per l'attuazione di eventuali deviazioni in caso di necessità dovute ad anomalie;
q) promuovere il territorio, anche con l'utilizzo di webcam o cameras on-line;
r) tutelare il patrimonio immobiliare e mobiliare dell'Ente;
s) abbinamento ad impianto antintrusione (attivato solo in assenza di personale);
t) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico da atti vandalici, danneggiamenti e furti;
u) tutelare gli utenti dei servizi dell'Ente;
v) tutelare il personale, a qualunque titolo, operante all'interno delle strutture dell'Ente;

z) diffondere riprese audio-video delle sedute del Consiglio comunale;

Il trattamento dei dati personali conseguente all'utilizzo del sistema di videosorveglianza trova un adeguato fondamento nelle **basi giuridiche** di seguito elencate.

Il trattamento dei dati personali (**comuni**) avviene in quanto:

N.A.	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (articolo 6, par. 1, lett. a) del RGPD)
N.A.	il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (articolo 6, par. 1, lett. b) del RGPD)
N.A.	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (articolo 6, par. 1, lett. c) del RGPD)
N.A.	il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (articolo 6, par. 1, lett. d) del RGPD)
X	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 (articolo 6, par. 1, lett. e) del RGPD)
N.A.	il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (articolo 6, par. 1, lett. f) del RGPD)
N.A.	Il trattamento è necessario per l'esecuzione di un compito di un'autorità competente per le finalità di cui all'articolo 1, comma 2 del D.Lgs. 51/2018 e si basa sul diritto dell'Unione europea o su disposizioni di legge o, nei casi previsti dalla legge, di regolamento che individuano i dati personali e le finalità del trattamento (articolo 5, comma 1 del D.Lgs. 51/2018)

Il trattamento dei 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 (**sensibili**) avviene in quanto:

N.A.	Non è previsto il trattamento di categorie particolari di dati personali
N.A.	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche (articolo 9, par. 2, lett. a) del RGPD)
N.A.	il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (articolo 9, par. 2, lett. b) del RGPD)
N.A.	il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (articolo 9, par. 2, lett. c) del RGPD)
N.A.	il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato (articolo 9, par. 2, lett. d) del RGPD)
N.A.	il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato (articolo 9, par. 2, lett. e) del RGPD)
N.A.	il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali (articolo 9, par. 2, lett. f) del RGPD)

X	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (articolo 9, par. 2, lett. g) del RGPD)
N.A.	il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (articolo 9, par. 2, lett. h) del RGPD)
N.A.	il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (articolo 9, par. 2, lett. i) del RGPD)
X	il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (articolo 9, par. 2, lett. j) del RGPD)
X	Il trattamento è necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento (articolo 7 del D.Lgs. 51/2018)
N.A.	Il trattamento è necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica (articolo 7 del D.Lgs. 51/2018)
N.A.	Il trattamento ha ad oggetto dati resi manifestamente pubblici dall'interessato (articolo 7 del D.Lgs. 51/2018)

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (**giudiziari**) avviene in quanto:

N.A.	Non è previsto il trattamento di dati a carattere giudiziario
X	Sotto il controllo dell'autorità pubblica
X	E' autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati

Il trattamento dei dati personali relativi ai **lavoratori** avviene in quanto:

X	Sottoscritto accordo ex art. 4 legge 300/1970 in materia di controlli a distanza attività lavoratori.

B.1.6. Necessità del trattamento

Il Titolare del trattamento ha valutato se questa **misura** fosse, in primo luogo, **idonea** al perseguimento delle finalità indicate e, in secondo luogo, se la misura fosse **adeguata** e **necessaria** per i propri scopi.

Stanti le caratteristiche territoriali, dimensionali ed organizzative dell'Ente, si è ritenuto necessario optare per un sistema di videosorveglianza in quanto le finalità indicate non potevano ragionevolmente essere perseguite con altri mezzi, meno intrusivi per i diritti e le libertà fondamentali dell'interessato.

Si è altresì stabilito di prevedere una **costante verifica** della necessità ed adeguatezza del sistema di videosorveglianza rispetto al perseguimento delle finalità dichiarate.

Circostanze che consentono o rendono necessario il ricorso al sistema di videosorveglianza:

X	Ampiezza del territorio di riferimento
X	Limitazione al numero di risorse umane impiegabili
X	Disposizioni normative generali o di settore in materia di circolazione stradale
X	Disposizioni normativa in materia di sicurezza urbana
X	Situazioni di pericolo connesse allo svolgimento di attività "di polizia"
X	Necessità di eseguire i controlli in particolari circostanze di tempo e di luogo
X	Necessità di monitoraggio del territorio ai fini di protezione civile

B.1.7. Soggetti del trattamento

B.1.7.1. Categorie di interessati

Il trattamento riguarda le seguenti categorie:

X	Persone fisiche presenti nell'area soggetta a monitoraggio e ripresa
X	Persone fisiche identificate a seguito dell'attività di accertamento delle violazioni amministrative
X	Persone fisiche identificate a seguito dell'attività di accertamento di reati
X	Persone fisiche in grado di riferire sulle circostanze relative alla infrazione od al sinistro stradale
X	Persone fisiche coinvolte in sinistri stradali

Il progetto prevede trattamenti su **larga scala** (il riferimento è a trattamenti su grandi quantità di dati, tenendo in considerazione il numero di soggetti interessati, il volume dei dati, l'ambito geografico, ecc.).

Numero approssimato di soggetti interessati anche in percentuale rispetto all'estensione geografica di riferimento: **non determinabile.**

B.1.7.2. Titolare del trattamento

Titolare del trattamento è: il **Comune di Serravalle Scrivia**

Il Titolare del trattamento rientra altresì nella definizione di "*Autorità competente*" quale risultante nell'**articolo 2, lettera g) del D.Lgs. 51/2018**:
1) qualsiasi autorità pubblica dello Stato, di uno Stato membro dell'Unione europea o di uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
2) qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;

Il titolare è soggetto con sede nell'Unione Europea; non necessita, pertanto, la nomina di un Rappresentante.

In ottemperanza all'obbligo contenuto nell'articolo 37 del RGPD e nell'articolo 28 del D.Lgs. 51/2018, il Titolare ha proceduto all'individuazione del **Responsabile della Protezione dei Dati Personali (RPD)**, alla comunicazione dei relativi dati di contatto al Garante per la protezione dei dati personali ed alla loro pubblicazione sul proprio sito web istituzionale.

Con riferimento al **personale** operante sotto la propria autorità, il Titolare ha previsto:
- l'identificazione di soggetti autorizzati al trattamento con assegnazione di specifiche istruzioni, ai sensi dell'**articolo 29 del RGPD e dell'articolo 19 del D.Lgs. 51/2018**;
- attribuzione ad uno o più soggetti determinati di specifici compiti e funzioni connessi al trattamento di dati personali, ai sensi dell'**articolo 2-quaterdecies del Codice privacy**.

Soggetti che operano sotto l'autorità del Titolare del trattamento:

X	Il Regolamento approvato dal Titolare prevede la figura del Responsabile del sistema complessivo di videosorveglianza, determinandone i compiti ed i poteri
X	Il Responsabile del sistema complessivo di videosorveglianza adotta un documento operativo contenente le decisioni in ordine alla gestione del sistema di videosorveglianza
X	Il personale autorizzato al trattamento è individuato ed istruito a cura del Responsabile del sistema complessivo di videosorveglianza

Responsabile del sistema di videosorveglianza

X	Comandante del corpo di Polizia Locale

Autorizzati al trattamento

X	Personale appartenente al corpo di Polizia Locale

Amministratore di sistema

X	Il Titolare ha designato un amministratore di sistema
N.A.	Il Titolare ha designato un amministratore di sistema all'interno della propria struttura organizzativa
N.A.	Il Titolare ha designato un amministratore di sistema all'interno della struttura organizzativa del Responsabile del trattamento
N.A.	L'amministratore di sistema è designato in relazione all'intero sistema informatico del Titolare

In ragione delle proprie caratteristiche soggettive e delle esigenze concrete il Titolare del trattamento può aderire a **standards internazionali** (ad. es. codici di condotta, certificazioni ISO, ecc.).

	SI	NO	Descrizione
Codici di condotta		**X**	
Certificazioni		**X**	

B.1.7.3. Contitolare del trattamento

L'**articolo 26 del RGPD** dispone che:
"*1. **Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento**. Essi determinano in modo trasparente, mediante un **accordo interno**, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.*
2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento".

L'**articolo 17 del D.Lgs. 51/2018** prevede che:
"*1. **Due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento sono contitolari del trattamento**.*
*2. I contitolari del trattamento determinano mediante **accordo** con modalità trasparenti gli ambiti delle rispettive responsabilità per l'osservanza delle norme di cui al presente decreto, salvo che detti ambiti siano determinati dal diritto dell'Unione europea o da disposizioni legislative o regolamentari.*
3. Con l'accordo di cui al comma 2 è designato il punto di contatto per gli interessati. Indipendentemente dalle disposizioni di tale accordo, l'interessato può esercitare i diritti nei confronti di e contro ciascun titolare del trattamento".

Nell'attuazione del progetto:

X	Non è previsto alcun rapporto di contitolarità

B.1.7.4. Responsabile del trattamento

L'**articolo 28 del RGPD** dispone che:
"*1. **Qualora un trattamento debba essere effettuato per conto del titolare del trattamento**, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*
(...)
*3. **I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*".

L'**articolo 18 del D.Lgs. 51/2018** dispone che:
"*1. **Qualora un trattamento debba essere effettuato per conto del titolare del trattamento**, quest'ultimo ricorre a responsabili del trattamento che garantiscono misure tecniche e organizzative adeguate ad assicurare la protezione dei dati personali e la tutela dei diritti dell'interessato.*
(...)
*3. L'esecuzione dei trattamenti da parte di un responsabile del trattamento è disciplinata da **un contratto o da altro atto giuridico** che prevede l'oggetto, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*".

Nell'attuazione del progetto:

X	Il trattamento dei dati per conto del Titolare è affidato ad un soggetto privato nel contesto di un servizio di assistenza e/o manutenzione
X	Il trattamento dei dati per conto del Titolare avviene in conseguenza dell'utilizzo di un servizio "Cloud"
X	Il trattamento dei dati per conto del Titolare avviene in conseguenza dell'accordo sottoscritto con McArthur Glenn (lettura targhe presso il centro commerciale)

Estremi identificativi del/i Responsabile/i e descrizione del trattamento:

B.1.7.5. Altro Responsabile del trattamento

L'**articolo 28 del RGPD** dispone che:
"*2. **Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta**, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.*
(…)
*4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, **su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, **gli stessi obblighi in materia di protezione dei dati** contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile*".

L'**articolo 18 del D.Lgs. 51/2018** dispone che:
"*(...)*
*2. Il responsabile del trattamento **non può ricorrere a un altro responsabile senza** preventiva autorizzazione scritta del titolare del trattamento.*
(...)".

Nell'attuazione del progetto:

N.A.	Non è consentito il ricorso ad altri responsabili (sub-responsabili)
N.A.	E' consentito il ricorso ad altri responsabili (sub-responsabili), previa autorizzazione generale
X	E' consentito il ricorso ad altri responsabili (sub-responsabili), previa autorizzazione specifica

B.2. VALUTAZIONE DELLA CONFORMITA' DEL TRATTAMENTO

Raccolte tutte le informazioni utili a identificare e censire il trattamento, si rende necessaria l'**analisi della necessità e della proporzionalità** del trattamento rispetto alle finalità.

B.2.1. verifica circa il rispetto del GDPR

Sono sottoposti a verifica i seguenti aspetti:

B.2.1.1. il trattamento rispetta i princìpi applicabili al trattamento dei dati personali (CAPO II del GDPR)

In relazione alle **finalità** del trattamento:

X	Le finalità sono chiaramente previste nel regolamento
X	Le finalità sono chiaramente indicate nell'informativa
X	Le finalità sono specificamente individuate in relazione a tutti i componenti del sistema
X	Il perseguimento delle finalità è conforme alla normativa di riferimento per il Titolare
X	I dati personali sono raccolti per le sole finalità indicate nell'informativa fornita all'Interessato del trattamento
X	Il trattamento risulta proporzionato e non eccedente rispetto le relative finalità. Infatti, lo stesso non concerne alcuna finalità ulteriore rispetto quelle esplicitate nell'informativa resa all'Interessato ai sensi dell'articolo 13 del RGPD

Le **basi giuridiche** del trattamento sono individuate e descritte.

In relazione alla **qualità** dei dati personali trattati

X	I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati
X	In fase di raccolta, esattezza ed aggiornamento conseguono automaticamente alle caratteristiche del trattamento

Adeguatezza, pertinenza e limitazione dei dati trattati:

X	Le videocamere sono posizione od orientate in modo da evitare la raccolta di notizie o immagini attinenti alla vita privata svolgentesi nell'abitazione o in un altro luogo di privata dimora, o nelle appartenenze di essi
X	Le videocamere fisse riprendono l'area sulla quale insistono 24 ore al giorno, 7 giorni su 7
	Le videocamere non consentono l'ascolto e la registrazione audio
X	Le videocamere consentono l'ascolto e la registrazione audio ma la relativa funzione è disattivata
	Le videocamere fisse sono brandeggiabili (anche solo parzialmente)
	Le videocamere mobili riprendono l'area oggetto di interesse unicamente al verificarsi di un evento rilevante (riconducibile alle finalità perseguite)
	Il sistema acquisisce mediante GPS la posizione geografica dell'infrazione
X	Esiste un sistema di controllo automatico, verifica ed aggiornamento data ed ora
	Il brandeggio manuale delle videocamere è oggetto di specifiche istruzioni
X	Il sistema consente di ingrandire digitalmente le immagini
X	E' possibile effettuare ricerche selettive tra le immagini raccolte
X	E' possibile l'utilizzo delle Zoom in relazione al sistema di videosorveglianza di contesto
	Vengono utilizzati sistemi di settaggio e/o oscuramento automatico
X	Il sistema di videosorveglianza di contesto e lettura targhe è configurato per eseguire la cancellazione automatica delle riprese al termine del previsto periodo di conservazione

X	L'analisi delle riprese rilevanti per un determinato evento comporta l'identificazione dei soli soggetti coinvolti e di coloro che possano riferire in merito alle circostanze dell'evento stesso
X	In relazione ad un evento rilevante, si procede ad estrazione della sola porzione di filmato necessaria alla ricostruzione dello stesso ed all'individuazione dei soggetti coinvolti
X	In caso di comunicazione ad altri soggetti è trasmessa la sola porzione di filmato necessaria alla ricostruzione dello stesso ed all'individuazione dei soggetti coinvolti
	Il sistema consente il mascheramento di soggetti che, pur presenti nelle riprese, non siano rilevanti per il caso
	In caso di richiesta di acquisizione dei filmati proveniente dall'Autorità giudiziaria o dalle Forze dell'ordine, i medesimi sono cancellati salvo che abbiano rilevanza per lo svolgimento di compiti e funzioni proprie del Titolare del trattamento

Sistemi di **analisi** video & alert:

X	Sono presenti sistemi di riconoscimento delle targhe dei veicoli ed abbinamento a black (white) lists
	Sono presenti sistemi di rilevazione di veicoli in movimento in direzione vietata o in sosta in zone proibite
	Sono presenti sistemi di rilevazione della tipologia (es. bus, camion, auto, ...), targa, modello, caratteristiche, velocità, dimensioni, autorizzazioni (es. trasporti pericolosi, ...) di veicoli
	Sono presenti sistemi di rilevazione di intrusione in ambienti interni od all'esterno
	Sono presenti sistemi di rilevazione di sagome di soggetti, oggetto, veicoli, ...
	Sono presenti sistemi di conteggio di persone presenti in un'area o che compiono determinate azioni
	Sono presenti sistemi di conteggio automatico di veicoli presenti o che transitano in un'area
	Sono presenti sistemi di tracciamento di soggetti, veicoli, ... (tracking)
	Sono presenti sistemi di rilevazione code di traffico
	Sono presenti sistemi di rilevazione velocità di veicoli, ...
	Sono presenti sistemi di rilevazione di veicoli in movimento in direzione vietata o in sosta in zone proibite (area pedonale urbana)
	Sono presenti sistemi di valutazione del livello di affollamento in zone critiche
	Sono presenti sistemi di conteggio automatico di veicoli presenti o che transitano in un'area
	Sono presenti sistemi di rilevazione di fumo e di incendio
	Sono presenti sistemi di rilevazione di cadute, con un possibile infortunio del soggetto coinvolto
	Sono presenti sistemi di rilevazione di oggetti abbandonati oppure rilevazione di oggetti sottratti
	Sono presenti sistemi di rilevazione di accecamento della videocamera o spostamento dalla posizione di riposo
	Sono presenti sistemi di rilevazione della presenza di un volto (face detection)
	Sono presenti sistemi di riconoscimento dei volti (face recognition)
	Sono presenti sistemi di attraversamento di una linea virtuale (trip wire)
	Sono presenti sistemi di rilevazione e gestione code ad uno sportello
	Sono presenti sistemi di rilevazione comportamenti anomali di soggetti (loitering)

L'**accesso alle immagini** registrate, da parte del personale dell'Ente, è effettuato:

X	d'ufficio, in caso di condotte illecite, di danno o di pericolo o per la rilevazione di sinistri stradali
X	su richiesta o segnalazione delle Forze dell'Ordine o dell'Autorità giudiziaria, in caso di condotte illecite di danno o di pericolo o per la rilevazione di sinistri stradali
X	su richiesta o segnalazione di cittadini ed utenti, in caso di condotte illecite di danno o di pericolo o per la rilevazione di sinistri stradali
	d'ufficio con cadenza periodica

In relazione alla **conservazione** dei dati personali trattati

X	il periodo di conservazione è limitato/idoneo ai fini per cui è stato effettuato il trattamento (per ciascuna categoria di dato)
X	È prevista una distinzione tra dati correnti e dati archiviati
	È prevista una forma di archiviazione automatica
X	È prevista una forma di cancellazione automatica
N.A.	La conservazione avviene in formato analogico
X	La conservazione avviene in formato digitale
	Sono previste attività di monitoraggio e verifica delle operazioni automatiche di cancellazione

Con particolare riferimento alle **figure soggettive** coinvolte:

X	Sono state individuate, autorizzate ed istruite le risorse umane deputate al trattamento
X	Sono stati individuati i Responsabili del trattamento ed è stato regolamentato il rapporto con il Titolare

Con particolare riferimento al **perimetro di conoscenza** delle informazioni:

X	Sono stati verificati i presupposti per la comunicazione dei dati personali
	Sono stati verificati i presupposti per il trasferimento dei dati personali extra UE (protezione equivalente)

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una **protezione equivalente**?
NO TRASFERIMENTO ALL'ESTERO

Con particolare riferimento alla **progettazione, realizzazione ed utilizzo** del sistema:

X	il Titolare del trattamento adotta misure organizzative e tecniche volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione (privacy by design)
X	il Titolare del trattamento integra nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati (privacy by design)
X	Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (privacy by default)

B.2.1.2. il trattamento rispetta i diritti degli interessati (CAPO III del Regolamento)

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

In linea generale, tutti i diritti sanciti dal RGPD si applicano al trattamento dei dati personali tramite sistemi videosorveglianza e di ripresa di immagini e video in generale.

Sono previste le seguenti modalità di **informazione** dell'Interessato:

X	Su supporto cartaceo, all'interno della modulistica in uso agli uffici
X	Sito web istituzionale
X	Cartellonistica
X	Segnaletica stradale
X	Le informazioni sono rese in modo da permettere all'Interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata

Rilevanza del **consenso** dell'Interessato

X	Non necessario
N.A.	Necessario
N.A.	Espresso in forma analogica
N.A.	Espresso in forma digitale

Possibilità di esercitare il diritto di **accesso**:

X	SI
N.A.	NO
X	NO, in relazione ai casi in cui non sia possibile individuare l'Interessato
X	NO, in relazione ai dati trattati in occasione del solo monitoraggio in tempo reale
X	NO, in relazione alle immagini e riprese video sottoposte a cancellazione
X	Regolamentazione delle modalità e procedura
X	Possibilità di escludere dall'accesso dati personali riferiti a terzi (mascheramento o crittografia)
X	E' prevista la verbalizzazione di quanto risultante dalla visione delle riprese, ad opera di un operatore di Polizia locale

Possibilità di esercitare il diritto alla **rettifica**:

N.A.	SI
X	NO

Possibilità di esercitare il diritto alla **integrazione**:

N.A.	SI
X	NO

Possibilità di esercitare il diritto alla **cancellazione** (diritto all'oblio):

X	SI
N.A.	NO
X	NO, in relazione ai dati trattati per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento

X	NO, in relazione ai casi in cui non sia possibile individuare l'Interessato
X	NO, in relazione ad immagini e riprese video sottoposte a cancellazione
X	NO, in relazione ai dati trattati in occasione del solo monitoraggio in tempo reale
X	Regolamentazione delle modalità e procedura per l'esercizio del diritto
X	Possibilità di offuscare l'immagine senza alcuna possibilità di recuperare successivamente i dati personali precedentemente contenuti nelle riprese
X	Previsione della necessità di informare qualunque soggetto al quale siano stati precedentemente comunicati i dati raccolti

Possibilità di esercitare il diritto alla **limitazione**:

X	SI
N.A.	NO
X	NO, in relazione ai casi in cui non sia possibile individuare l'Interessato
X	NO, in relazione ai dati trattati in occasione del solo monitoraggio in tempo reale
X	NO, in relazione ad immagini e riprese video sottoposte a cancellazione
X	Regolamentazione delle modalità e procedura per l'esercizio del diritto
X	Previsione della necessità di informare qualunque soggetto al quale siano stati precedentemente comunicati i dati raccolti

Possibilità di esercitare il diritto alla **portabilità**:

X	NO, in quanto il trattamento non si basa sul consenso dell'Interessato o su di un contratto

Possibilità di esercitare il diritto alla **opposizione**:

N.A.	SI
X	NO, in quanto sussistono motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato
X	NO, in quanto il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
X	Regolamentazione delle modalità e procedura per l'esercizio del diritto

Diritto a non essere sottoposto ad un **processo decisionale automatizzato**:

N.A.	SI
X	NO, in conseguenza dell'uso del sistema di videosorveglianza l'interessato non è sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione
N.A.	Regolamentazione delle modalità e procedura per l'esercizio del diritto
X	Regolamentazione delle modalità e procedura per garantire l'intervento umano da parte del Titolare del trattamento
N.A.	Regolamentazione delle modalità e procedura per consentire all'Interessato di esprimere la propria opinione e di contestare la decisione

B.2.1.3. Il trattamento rispetta la normativa di settore, rilevante in tema di videosorveglianza

L'impiego di sistemi di videosorveglianza è previsto e regolamentato da differenti fonti normative.
Il Titolare ritiene di essere soggetto e di aver rispetto le seguenti prescrizioni normative:

X	Decreto-legge 16/07/2020, n. 76
X	Decreto-legge 18 aprile 2019, n. 32

X	Decreto-legge 4 ottobre 2018, n. 113
X	Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15
X	Decreto-legge 20 febbraio 2017, n. 14
X	Decreto Ministero dell'Interno 24 maggio 2017
X	Direttiva Ministero dell'Interno 558/SICPART/421.2/224632 del 02.03.2012
X	Decreto Ministero dell'Interno 15 settembre 2009, n. 154
X	Decreto-legge 23 febbraio 2009, n. 11
X	Decreto Ministero dell'Interno 5 agosto 2008
X	Decreto Ministero dell'Interno 6 giugno 2005
X	Decreto Legislativo 7 marzo 2005, n. 82
X	Decreto-legge 24 febbraio 2003, n. 28
X	Decreto-legge 20 giugno 2002, n. 121
X	Decreto del Presidente della Repubblica 22 giugno 1999, n. 250
X	Decreto del Presidente della Repubblica 16 dicembre 1992, n. 495
X	Decreto Legislativo 30 aprile 1992, n. 285
X	Decreto Ministero dell'Interno 4 marzo 1987, n. 145
X	Legge 24 novembre 1981, n. 689
X	Legge 20 maggio 1970, n. 300

B.2.2. esito della verifica di conformità

Prima di procedere oltre con la Valutazione d'impatto, occorre constatare la conformità del trattamento sotto il profilo del rispetto alla normativa di protezione dei dati personali.
Conclusivamente, il trattamento si presenta:

X	**CONFORME** ALLA NORMATIVA DI PROTEZIONE DEI DATI PERSONALI e, pertanto, si può procedere con l'analisi che segue
N.A.	**NON CONFORME** ALLA NORMATIVA DI PROTEZIONE DEI DATI PERSONALI e, pertanto, si rende necessario sottoporlo ad ulteriore verifica

B.3. VALUTAZIONE DELLA OBBLIGATORIETÀ DELLA DPIA

Si rende a questo punto necessario verificare se l'esecuzione della presente DPIA sia resa necessaria in conseguenza di un obbligo normativo ovvero se essa sia svolta a seguito di una decisione discrezionale del Titolare del trattamento.

Circa una eventuale **NON NECESSITA'** di effettuare una DPIA:

N.A.	Il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1 del RGPD)
N.A.	Esiste un trattamento avente le medesime caratteristiche quello analizzato e già sottoposto positivamente a DPIA che renda non necessario ripeterla
N.A.	Il trattamento ha come base legale il diritto della Unione Europea o dello Stato membro e la DPIA è già stata realizzata in questo contesto
N.A.	Sulla medesima tipologia di trattamento è stata effettuata una verifica o un controllo da parte del Garante per la protezione dei dati personali che consente lo svolgimento del trattamento senza ulteriori DPIA
N.A.	Il trattamento rientra nell'elenco facoltativo (stabilito dall'Autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5)
N.A.	Non vi sono ragioni per ritenere la DPIA non necessaria

Sebbene non necessaria, il Titolare del trattamento ha ritenuto di procedere comunque con l'effettuazione della DPIA?

N.A.	SI
N.A.	NO

Di seguito sono elencate le fattispecie nelle quali sussiste l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati personali.
Per ciascuna di esse è precisato se l'individuazione sia avvenuta ad opera del Gruppo di lavoro "Articolo 29" (Art. 29 WP) o ad opera del Garante per la Protezione dei Dati Personali (GPDP).
Circa la **NECESSITA'** di effettuare una DPIA:

N.A.	Non è possibile stabilire con sufficiente evidenza se il trattamento presenta o meno rischi elevati per gli interessati
N.A.	Valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche (articolo 35 del RGPD)
N.A.	Trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR (articolo 35 del RGPD)
X	Sorveglianza sistematica su larga scala di una zona accessibile al pubblico (articolo 35 del RGPD)
N.A.	Valutazione o assegnazione di un punteggio, incluse la profilazione e la predizione, in particolare a partire da aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato (Considerando 71 e 91) (Linee Guida del WP29)
N.A.	Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a) (Linee Guida del WP29)

N.A.	Monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare soggetti interessati, inclusi i dati raccolti attraverso un controllo sistematico di una zona accessibile al pubblico (articolo 35, paragrafo 3, lettera c) (Linee Guida del WP29)
X	Trattamento di dati particolari: si tratta delle categorie particolari di dati ai sensi dell'articolo 9 del GDPR oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10 (Linee Guida del WP29)
X	Trattamenti di dati elaborati su larga scala (il WP29 raccomanda che i seguenti fattori, in particolare, siano considerati per determinare se il trattamento è effettuato su larga scala: a. il numero di persone interessate, come numero specifico o come percentuale della popolazione di riferimento; b. il volume dei dati e / o la gamma di diversi elementi di dati in corso di elaborazione; c. la durata, o la permanenza, dell'attività di elaborazione dati; d. l'estensione geografica delle attività di elaborazione) (Linee Guida del WP29)
N.A.	Creazione di corrispondenze o combinazione di insiemi di dati, ad esempio provenienti da due o più trattamenti effettuati per scopi diversi e / o da altri titolari in modo tale da superare le ragionevoli aspettative dell'interessato (Linee Guida del WP29)
N.A.	Trattamenti di dati relativi a interessati vulnerabili (Considerando 75): il trattamento di questo tipo di dati può richiedere una DPIA a causa del maggiore squilibrio di potere tra interessato e titolare del trattamento, nel senso che il singolo può non essere in grado di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i minori, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento (Linee Guida del WP29)
N.A.	Utilizzi innovativi o applicazione di soluzioni tecnologiche o organizzative, come la combinazione fra l'uso di impronte digitali e il riconoscimento del volto per un migliore controllo di accesso fisico, ecc. (Linee Guida del WP29)
N.A.	Trattamenti che impediscono agli interessati di esercitare un diritto o utilizzare un servizio o un contratto" (ad es. lo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento) (articolo 22 e Considerando 91) (Linee Guida del WP29)
N.A.	Trattamento soggetto a un codice di condotta che richiede lo svolgimento della DPIA (Linee Guida del WP29)
N.A.	Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (Garante privacy, provv. 467 del 11 ottobre 2018)
N.A.	Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi) (Garante privacy, provv. 467 del 11 ottobre 2018)
X	Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc. (Garante privacy, provv. 467 del 11 ottobre 2018)

N.A.	Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti) (Garante privacy, provv. 467 del 11 ottobre 2018)
X	Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8) (Garante privacy, provv. 467 del 11 ottobre 2018)
N.A.	Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo (Garante privacy, provv. 467 del 11 ottobre 2018)
X	Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 (Garante privacy, provv. 467 del 11 ottobre 2018)
X	Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche (Garante privacy, provv. 467 del 11 ottobre 2018)
N.A.	Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment) (Garante privacy, provv. 467 del 11 ottobre 2018)
X	Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse (Garante privacy, provv. 467 del 11 ottobre 2018)
N.A.	Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento (Garante privacy, provv. 467 del 11 ottobre 2018)
N.A.	Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento (Garante privacy, provv. 467 del 11 ottobre 2018)

La necessità di effettuare la DPIA risulta palese nell'ottica della previsione di cui all'articolo 35 del RGPD, per il fatto che si tratta di "**sorveglianza sistematica su larga scala di una zona accessibile al pubblico**". In particolare:

✓ "**sistematica**": il trattamento avviene mediante un sistema ed in modo predeterminato, organizzato e metodico. Non è possibile per gli interessati evitare di essere soggetti a tale trattamento nel momento in cui gli stessi accedono alle aree videosorvegliate;

✓ "**su larga scala**": il trattamento, essendo svolto con molte telecamere, in modo continuativo e su aree pubbliche frequentate, ha ad oggetto una notevole quantità di dati personali riferiti ad un ampio numero di soggetti interessati (abitanti, residenti, turisti, automobilisti, pedoni, personale della Pubblica Amministrazione e aziende private);

✓ "**in zone accessibili al pubblico**" perché le aree oggetto di rilevazione sono aree pubbliche o di pubblico passaggio e quindi accessibili a chiunque.

Conclusivamente si può affermare che il trattamento dei dati personali attraverso l'impiego di un sistema di videosorveglianza **presenti un rischio elevato per i diritti e le libertà delle persone fisiche**.

C. MISURE DI SICUREZZA

In questa sezione sono descritte le misure di sicurezza, **esistenti o pianificate** che contribuiscono alla sicurezza dei dati personali.

Esse sono ripartite in diverse categorie, sulla scorta della classificazione suggerita da **ENISA**. Per ciascuna categoria è altresì riportata la corrispondente categoria utilizzata dallo standard **ISO/IEC 27001:2013**.

INDICE DELLE MISURE		
ENISA		**ISO**
A. Politiche di sicurezza e procedure per la protezione dei dati personali		A.5 Politiche per la sicurezza delle informazioni
B. Ruoli e responsabilità		A.6.1.1 Ruoli e responsabilità per la sicurezza delle informazioni
C. Politica controllo accessi		A.9.1.1 Politica di controllo degli accessi
D. Gestione risorse e degli asset		A.8 Gestione degli asset
E. Change management		A.12.1 Procedure operative e responsabilità
F. Responsabile del trattamento (Data processors)		A.15 Relazione con i fornitori
G. Gestione degli incidenti / Violazione dei dati personali		A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni
H. Business continuity		A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa
I. Riservatezza del personale		A.7 Sicurezza delle risorse umane
J. Formazione		A.7.2.2 Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni
K. Controllo accessi e autenticazione		A.9 Controllo degli accessi
L. Logging e monitoraggio		A.12.4 Raccolta dei log e monitoraggio
M. Sicurezza Server e Database		A.12 Sicurezza delle attività operative
N. Sicurezza desktop/laptop/mobile		A.14.1 Requisiti di sicurezza dei sistemi informativi
O. Network/Communication security		A.13 Sicurezza delle comunicazioni
P. Backup		A.12.3 Backup
Q. Dispositivi portatili		A.6.2 Dispositivi portatili e telelavoro
R. Sicurezza del ciclo di vita delle applicazioni		A.12.6 Gestione delle vulnerabilità tecniche A.14.2 Sicurezza nei processi di sviluppo e supporto
S. Cancellazione/eliminazione dei dati		A.8.3.2 Dismissione dei supporti A.11.2.7 Dismissione sicura o riutilizzo delle apparecchiature
T. Sicurezza fisica		A.11 Sicurezza fisica e ambientale

A. Politiche di sicurezza e procedure per la protezione dei dati personali:

X	A.1 - L'organizzazione dovrebbe documentare la propria politica in merito all'elaborazione dei dati personali come parte della sua politica di sicurezza delle informazioni
X	A.2 - La politica di sicurezza dovrebbe essere riesaminata e aggiornata, se necessario, su base annuale
X	A.3 - L'organizzazione dovrebbe documentare una politica di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La politica dovrebbe essere approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate
X	A.4 - La politica di sicurezza dovrebbe almeno fare riferimento a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali,

	per i responsabili del trattamento dei dati o per le altre terze parti coinvolte nel trattamento dei dati personali
N.A.	A.5 - Dovrebbe essere creato e mantenuto un inventario di politiche / procedure specifiche relative alla sicurezza dei dati personali, basato sulla politica generale di sicurezza
N.A.	A.6 - La politica di sicurezza dovrebbe essere riesaminata e aggiornata, se necessario, su base semestrale

Misure specifiche:

X	Adozione di un Modello Organizzativo
X	Adozione di un Regolamento per la gestione del servizio di videosorveglianza
X	Prevista l'individuazione di un Responsabile del sistema complessivo di videosorveglianza
X	Adozione di istruzioni specifiche in capo ai soggetti autorizzati al trattamento in questione
X	Adozione di istruzioni generali in tema di protezione dei dati personali
X	Le autorizzazioni al trattamento (e le relative autenticazioni) sono riconosciute in quanto necessarie allo svolgimento dei compiti e delle mansioni assegnate al personale
X	Le autorizzazioni al trattamento (e le relative autenticazioni) sono riconosciute ed assegnate con scadenza temporale, soggetta a revisione periodica

B. Ruoli e responsabilità:

X	B.1 - I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza
X	B.2 - Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, devono essere chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne
X	B.3 - Dovrebbe essere effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza
X	B.4 - Il responsabile della sicurezza dovrebbe essere nominato formalmente (in modo documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati
X	B.5 - Doveri e aree di responsabilità che possono essere in conflitto, ad esempio i ruoli di responsabile della sicurezza, auditor e DPO, dovrebbero essere considerati separati per ridurre le opportunità di modifiche non autorizzate o non intenzionali o di uso improprio di dati personali

C. Politica controllo accessi:

X	C.1 - I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza
X	C.2 - Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali
X	C.3 - La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi) dovrebbe essere chiaramente definita e documentata
X	C.4 - I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale

D. Gestione risorse e degli asset:

X	D.1 - L'organizzazione dovrebbe disporre di un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro potrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. server, workstation), posizione (fisica o elettronica). Ad una persona specifica dovrebbe essere assegnato il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT)
X	D.2 - Le risorse IT dovrebbero essere riesaminate e aggiornate regolarmente
X	D.3 - I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati
N.A.	D.4 - Le risorse IT dovrebbero essere riesaminate e aggiornate su base annuale

E. Gestione delle modifiche:

X	E.1 - L'organizzazione deve assicurarsi che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, responsabile IT o sicurezza). Questo processo dovrebbe essere monitorato regolarmente
N.A.	E.2 - Lo sviluppo del software dovrebbe essere eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire l test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non è possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test
X	E.3 - Dovrebbe essere presente una politica dettagliata e documentata di gestione dei cambiamenti. Dovrebbe includere: un processo per l'introduzione dei cambiamenti, i ruoli / utenti che hanno i diritti di cambiamento, le tempistiche per l'introduzione dei cambiamenti. La politica di gestione dei cambiamenti dovrebbe essere regolarmente aggiornata

Misure specifiche:

X	Esiste un censimento dei sistemi di rilevazione installati
X	Esiste un processo strutturato e formalizzato per l'installazione, l'assegnazione, restituzione e dismissione dei beni (hardware, software)
	Le videocamere installate sono geolocalizzate
X	Esistono planimetrie con la localizzazione delle videocamere installate
X	L'intero impianto e le sue componenti sono sottoposti a verifica periodica al fine di identificare inefficienze e pianificare ampliamenti o riduzioni
X	Esiste un inventario aggiornato di tutte le componenti hardware e software del sistema di videosorveglianza
X	Vengono eseguiti di collaudi formali e test, per assicurare funzionalità, conformità tecnica e requisiti di sicurezza in caso di acquisizione, sviluppo, manutenzione dei sistemi IT, prima di rendere operativi i sistemi
X	Non è ammessa l'installazione di software non autorizzato e esistono strumenti per identificare e rimuovere periodicamente software installato dal PC degli utenti
X	I programmi contro i software dannosi sono costantemente aggiornati

F. Responsabile del trattamento (Data processor):

	F.1 - Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcer) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione
	F.2 - E' necessario predisporre clausole contrattuali per le quali al rilevamento di una violazione dei dati personali, il responsabile del trattamento informi il titolare del trattamento senza indebiti ritardi

	F.3 - Fra il titolare del trattamento dei dati e il responsabile del trattamento dei dati dovrebbero essere formalmente concordati requisiti formali e obblighi. Il Responsabile del trattamento dovrebbe fornire prove documentate sufficienti di conformità
	F.4 - L'organizzazione Titolare del trattamento dei dati dovrebbe verificare regolarmente la conformità del Responsabile del trattamento al livello concordato di requisiti e obblighi
	F.5 - Il personale del responsabile del trattamento che elabora dati personali deve essere soggetto a specifici accordi documentati di riservatezza / non divulgazione

Misure specifiche:

X	E' prevista una procedura di valutazione dei responsabili prima dell'affidamento delle operazioni di trattamento
X	E' predisposto uno specifico testo contrattuale (DPA) per la regolamentazione dei rapporti Titolare/Responsabile
X	Gli accessi ai sistemi informativi da parte dei Responsabili avvengono su richiesta del Titolare e sono presidiati
X	Gli interventi di manutenzione/assistenza sulle componenti hardware e software del sistema avvengono su richiesta e sono presidiati dal personale del Titolare
X	Il personale operante nella struttura del Responsabile che accede alle registrazioni è qualificato come ausiliario di PS/PG
X	Apposito personale appartenente alla struttura del Responsabile è designato Amministratore di sistema
X	E' fatto obbligo al Responsabile di procedere alla individuazione di un Amministratore di sistema
X	E' fatto obbligo al Responsabile di procedere alla nomina del Responsabile della protezione dei dati personali (RPD o DPO)
X	Il ricorso a sub-responsabili è consentito su autorizzazione preventiva del Titolare

G. Gestione degli incidenti / violazione dei dati personali (documento "Policy Gestione incidenti di sicurezza", in attesa di deliberazione di Giunta Comunale)

X	G.1 - È necessario definire un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali
X	G.2 - Le violazioni dei dati personali devono essere segnalate immediatamente alla Direzione. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR
X	G.3 - Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli
X	G.4 - Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite

Misure specifiche:

X	Adozione di una Data Breach Policy
X	Assegnazione compiti e responsabilità specifiche
X	Previsione di specifici obblighi per Contitolari/Responsabili
X	Previsione di una formazione specifica per il personale in materia di sicurezza e violazione di dati personali
X	Istituzione di un registro delle violazioni di dati personali
X	Istituzione di un registro degli incidenti non costituenti violazioni di dati personali

H. Business continuity:

	H.1 - L'organizzazione dovrebbe stabilire le procedure e i controlli principali da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema informatico che elabora i dati personali (in caso di incidente / violazione dei dati personali)
	H.2 - Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli
	H.3 - Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali
	H.4 - Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali
	H.5 - Si dovrebbe prendere in considerazione una struttura alternativa, a seconda dell'organizzazione e dei tempi di inattività accettabili del sistema IT

Misure specifiche:

X	Le apparecchiature collocate presso la/e sala/e di controllo" dispongono di alimentazione di continuità e di emergenza
X	E' previsto il monitoraggio manuale e periodico del funzionamento del sistema
X	Esiste un contratto di manutenzione/assistenza a copertura di guasti ed avarie alle componenti fisiche o informatiche
X	Esiste un contratto di manutenzione/assistenza a copertura di eventi atmosferici
X	Esiste un contratto di manutenzione/assistenza a copertura di atti vandalici od intenzionali
X	Esiste un contratto di assistenza a copertura di esigenze legate agli utilizzatori (modifiche di autorizzazioni, nuovi ingressi, revoche, ...)
x	Il contratto di manutenzione/assistenza prevede tempi di intervento su chiamata
x	Il contratto di manutenzione/assistenza prevede tempi di ripristino del funzionamento del sistema
x	Il contratto di manutenzione/assistenza prevede frequenze periodiche di verifica
X	Le videocamere sono dotate di sistemi di antimanomissione (perdita segnale, offuscamento, modifica inquadratura, …)
X	Il sistema è dotato di un software di monitoraggio della connessione delle telecamere
X	Le videocamere sono protette dall'azione degli agenti atmosferici

I. Riservatezza del personale:

X	I.1 - L'organizzazione dovrebbe garantire che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante il processo di pre-assunzione e / o inserimento
X	I.2 - Prima di assumere i propri compiti, il personale dovrebbe essere invitato a riesaminare e concordare la politica di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione
X	I.3 - Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale)

Misure specifiche:

X	Il personale è tenuto al segreto d'ufficio
X	Il personale che ha accesso alle immagini ha la qualifica di Ufficiale/Agente di Polizia Giudiziaria

J. Formazione del personale:

X	J.1 - L'organizzazione dovrebbe garantire che tutto il personale sia adeguatamente informato sui controlli di sicurezza del sistema informatico relativi al suo lavoro quotidiano. Il personale coinvolto nel trattamento dei dati personali dovrebbe inoltre essere adeguatamente informato in merito ai

	requisiti in materia di protezione dei dati e agli obblighi legali attraverso regolari campagne di sensibilizzazione
X	J.2 - L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati
X	J.3 - Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale

Misure specifiche:

X	E' previsto un piano generale di formazione in materia di protezione dei dati personali
X	E' previsto un percorso formativo specifico per l'utilizzo di sistemi di videosorveglianza
X	E' previsto un percorso formativo specifico per la gestione dei rapporti con le Forze dell'ordine e l'Autorità giudiziaria
X	E' previsto un percorso formativo specifico per la gestione dei rapporti con gli interessati ed altri soggetti legittimati all'accesso in virtù di normativa specifica (Legge 241/90, 391-quater Cpp, ...)

K. Controllo accessi IT e autenticazione:

X	K.1 - Dovrebbe essere attuato un sistema di controllo accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, il riesame e l'eliminazione degli account degli utenti
X	K.2 - L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità
X	K.3 - Dovrebbe essere presente un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di user-id e password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità
	K.4 - Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile)
	K.5 - Una politica specifica per la password dovrebbe essere definita e documentata. La politica deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili
	K.6 - Le password degli utenti devono essere archiviate in formato "hash"
	K7 - L'autenticazione a due fattori dovrebbe preferibilmente essere utilizzata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
	K.8 - Dovrebbe essere utilizzata l'autenticazione dei dispositivi per garantire che l'elaborazione dei dati personali venga eseguita solo attraverso risorse di rete specifiche

Misure specifiche:

	Il sistema informativo dedicato alla videosorveglianza è separato (fisicamente o logicamente) rispetto al sistema complessivo del Titolare
X	Il traffico da e verso il sistema di videosorveglianza è monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni
X	L'accesso tramite internet al sistema di videosorveglianza avviene in modalità sicure tramite protocolli crittografici (TLS/SSL)
X	Gli accessi e l'utilizzo dei sistemi informativi sono presidiati da regole e procedure di autorizzazione ed autenticazione
X	Ciascun operatore dispone di credenziali di autenticazione individuali

X	E' vietata la condivisione di credenziali di autenticazione individuali
X	I software prevedono time out di sessione;
X	Il titolare verifica costantemente i diritti di accesso degli utenti; le credenziali sono disattivate in caso di perdita della qualità che consente all'utente l'accesso ai dati
X	Il personale è istruito in relazione alla creazione ed all'uso di password sicure
X	L'operatore è adeguatamente edotto sulla necessità di bloccare lo schermo in caso di allontanamento dalla postazione
X	Sono previste regole e procedure specifiche per l'accesso remoto al sistema (VPN, identificazione IP, ...)

L. Logging e monitoraggio:

	L.1 - I log devono essere attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione)
	L.2 - I log devono essere registrati con marcatura temporale (timestamp) e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento
	L.3 - È necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti
	L.4 - Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei log. Anche l'accesso ai log deve essere registrato oltre al monitoraggio per rilevare attività insolite
	L.5 - Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi

Misure specifiche:

X	A ciascun utente è assegnato un codice univoco che lo identifica all'interno dei log

M. Sicurezza Server e Database:

	M.1 - I database e application server devono essere configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente
	M.2 - I database e application server devono elaborare solo i dati personali che sono effettivamente necessari per l'elaborazione al fine di raggiungere i propri scopi di elaborazione
	M.3 - Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'uso di software o hardware
	M.4 - È necessario prendere in considerazione la crittografia delle unità di archiviazione
	M.5 - Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione dei dati dagli identificatori diretti per evitare il collegamento all'interessato senza ulteriori informazioni
	M.6 - Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le authorized queries, il privacy preserving data base querying, la searchable encryption, ecc.

Misure specifiche:

X	I dati conservati in relazione a procedimenti civili, amministrativi e penali sono crittografati
X	I dati raccolti dalle foto-trappole sono crittografati
X	I dati raccolti dalle Body-Cam sono crittografati
N.A.	I dati raccolti dalle Dash-Cam sono crittografati
N.A.	I dati raccolti dai Droni sono crittografati
X	Il sistema di registrazione dei filmati e delle immagini è digitale
X	Il sistema di registrazione dei filmati è analogico

N.A.	I dati raccolti per esigenza di addestramento del sistema sono anonimizzati mediante oscuramento delle porzioni identificative delle immagini
N.A.	I dati conservati in relazione a procedimenti civili, amministrativi e penali sono soggetti a meta-datazione nel rispetto delle Linee Guida AgID in materia di formazione, gestione e conservazione dei documenti amministrativi
X	L'accesso ai dati conservati è soggetto a regole e procedura che consentano di limitarlo a favore dei soli soggetti autorizzati
X	Adozione di tecniche e strumenti per tenere traccia delle responsabilità connesse al compimento di specifiche operazioni, quali l'estrazione delle immagini, la meta-datazione, la copia, ... (c.d. watermarking)

N. Sicurezza desktop/laptop/mobile:

	N.1 - Gli utenti non dovrebbero essere in grado di disattivare o aggirare le impostazioni di sicurezza
	N.2 - Le applicazioni antivirus e le relative signatures devono essere configurate su base settimanale
	N.3 - Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate
	N.4 - Il sistema dovrebbe avere time-out di sessione quando l'utente non è stato attivo per un certo periodo di tempo
	N.5 - Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema devono essere installati regolarmente
	N.6 - Le applicazioni antivirus e le relative firme devono essere configurate su base giornaliera
	N.7 - Non dovrebbe essere consentito il trasferimento di dati personali da workstation a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni)
	N.8 - Le workstation utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire l'elaborazione, la copia e il trasferimento non autorizzati dei dati personali archiviati
	N.9 - La crittografia del disco completo dovrebbe essere abilitata su tutte le unità della workstation

O. Network/Communication security:

	O.1 - Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL)
	O.2 - L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e processi specifici. Dovrebbe essere protetto da meccanismi di crittografia
	O.3 - In generale, l'accesso remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti
	O.4 - Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni
	O.5 - La connessione a Internet non dovrebbe essere consentita ai server e alle workstation utilizzate per il trattamento dei dati personali
	O.6 - La rete IT dovrebbe essere separata dalle altre reti del titolare
	O.7 - L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali preautorizzati utilizzando tecniche come il MAC filtering o il Network Access Control (NAC)

Misure specifiche:

X	La connessione delle videocamere al sistema di videosorveglianza avviene mediante apparati wireless (umts, gsm, wi-fi, radio, ...)

X	La connessione delle videocamere al sistema di videosorveglianza avviene mediante sistema misto (wireless e cavo)
X	Gli interventi di assistenza avvengono su richiesta del Titolare
X	I soggetti interni che hanno accesso al sistema informativo sono qualificati come "Ausiliari di PG"
X	Il trasferimento al sistema di registrazione delle immagini registrate dalle videocamere avviene in tempo reale
X	E' previsto l'utilizzo di tecnologia VPN con crittografia
X	E' previsto l'utilizzo di protocolli di comunicazione con crittografia (https, ssl, tls, ...)
X	Gli elaboratori utilizzati dal sistema dispongono di protezione da malware
X	La rete è dotata di firewall

P. Backup:

	P.1 - Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità
	P.2 - Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine
	P.3 - L'esecuzione dei backup deve essere monitorata per garantire la completezza
	P.4 - I backup completi devono essere eseguiti regolarmente
	P.5 - I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati
	P.6 - I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera
	P.7 - Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine
	P.8 - Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare dei dati

Misure specifiche:

X	L'archivio delle registrazioni correnti non è sottoposto a Backup
N.A.	L'archivio delle registrazioni correnti è sottoposto a Backup con criteri di cancellazione automatica
X	E' previsto il backup delle sole registrazioni conservate a seguito di estrazione, separatamente rispetto alla conservazione generale del patrimonio documentale del Titolare
X	E' previsto il backup delle sole registrazioni conservate a seguito di estrazione, integrato nel sistema di conservazione generale del patrimonio documentale del Titolare

Q. Dispositivi portatili:

	Q.1 - Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo
	Q.2 - I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati
	Q.3 - I dispositivi mobili dovrebbero essere soggetti alle stesse procedure di controllo degli accessi (al sistema IT) delle altre apparecchiature terminali
	Q.4 - I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti
	Q.5 - L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali su un dispositivo mobile compromesso
	Q.6 - I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso software containers sicuri
	Q.7 - I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso
	Q.8 - Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori

	Q.9 - I dati personali memorizzati sul dispositivo mobile (come parte delle operazioni di elaborazione dei dati dell'organizzazione) devono essere cifrati

Misure specifiche:

X	L'assegnazione di dispositivi mobili al personale avviene in modo specifico e con assegnazione di specifiche istruzioni
X	L'estrazione delle riprese contenute in dispositivi mobili assegnati individualmente avviene da personale autorizzato nel rispetto di procedure specifiche

R. Sicurezza del ciclo di vita delle applicazioni:

N.A.	R.1 - Durante il ciclo di vita dello sviluppo si devono seguire le migliori pratiche, lo stato dell'arte e pratiche, framework o standard di sicurezza ben noti
N.A.	R.2 - Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo
N.A.	R.3 - Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET Privacy Enhancing Technologies)) dovrebbero essere adottate in analogia con i requisiti di sicurezza
N.A.	R.4 - Dovrebbero essere seguiti standard e pratiche di codifica sicure
N.A.	R.5 - Durante lo sviluppo, devono essere eseguiti test e convalida rispetto all'implementazione dei requisiti di sicurezza iniziali
N.A.	R.6 - I vulnerability assessment, i penetration test applicativi e dell'infrastruttura dovrebbero essere eseguiti da una terza parte fidata prima del passaggio in ambiente di produzione. Il passaggio non può avvenire a meno che non sia raggiunto il livello di sicurezza richiesto
N.A.	R.7 - Devono essere eseguiti penetration test periodici
N.A.	R.8 - Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi IT utilizzati
N.A.	R.9 - Le patch software dovrebbero essere testate e valutate prima di essere installate in ambiente di produzione

S. Cancellazione/eliminazione dei dati:

X	S.1 - Software di sovrascrittura dovrebbe essere usato su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), i supporti dovrebbero essere distrutti fisicamente
X	S.2 - È necessario eseguire la triturazione di carta e supporti portatili utilizzati per memorizzare i dati personali
N.A.	S.3 - Più passaggi di software di sovrascrittura devono essere eseguiti su tutti i supporti prima di essere smaltiti
N.A.	S.4 - Se i servizi di terzi sono utilizzati per eliminare in modo sicuro i supporti o i documenti cartacei, è necessario stipulare un contratto di servizio e produrre un attestato di distruzione, a seconda dei casi
N.A.	S.5 - Dopo la cancellazione dei dati con un software, devono essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda dei casi, dovrebbe essere considerata anche la distruzione fisica
N.A.	S.6 - Se una terza parte, quindi un responsabile del trattamento, viene utilizzata per la distruzione di supporti o documenti cartacei, il processo si potrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento dei dati personali

Misure specifiche:

X	Il sistema è dotato di una funzione di cancellazione automatica temporizzata delle immagini e delle riprese video
X	La cancellazione dei dati avviene mediante sovrascrittura
X	Sono previste regole e procedure per la cancellazione delle registrazioni erronee o accidentali, acquisite da sistemi mobili (body-cam, dash-cam e droni)

T. Sicurezza fisica:

X	T.1 - Il perimetro fisico dell'infrastruttura IT non dovrebbe essere accessibile da personale non autorizzato
X	T.2 - L'identificazione chiara, tramite mezzi appropriati, ad es. badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbe essere stabilita, a seconda dei casi
X	T.3 - Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi devono essere mantenuti e monitorati in modo sicuro
X	T.4 - I sistemi di rilevamento antintrusione dovrebbero essere installati in tutte le zone di sicurezza
X	T.5 - Le barriere fisiche dovrebbero, se del caso, essere costruite per impedire l'accesso fisico non autorizzato
X	T.6 - Le aree non usate dovrebbero essere fisicamente bloccate e periodicamente riesaminate
X	T.7 - Un sistema antincendio automatico, un sistema di climatizzazione dedicato e chiuso e un gruppo di continuità (UPS) dovrebbero essere usati nella sala server
X	T.8 - Il personale di supporto esterno deve avere accesso limitato alle aree protette

Misure specifiche:

X	E' individuato un apposito locale od area come "sala operativa" o "centrale di controllo"
X	L'accesso alla "sala operativa" è consentito solamente al personale autorizzato
X	Gli accessi e la permanenza nella "sala operativa" sono registrati in apposito registro (elettronico)
	Gli accessi alla "sala operativa" sono videosorvegliati
X	Il locale alla "sala operativa" è sempre presidiato da un operatore
X	Gli ingressi alla "sala operativa" sono protetti da chiave (fisica o elettronica)
X	Le finestre/porte della "sala operativa" sono dotate di barriere antiintrusione
X	Il locale alla "sala operativa" è dotato di impianto di allarme
X	Sono previsti impianti per l'estinzione degli incendi
X	E' presente un sistema di spegnimento incendio non ad acqua
	Le uscite di sicurezza della "sala operativa" sono allarmate
X	L'accesso del personale esterno alla "sala operativa" avviene solo su richiesta ed è presidiato da un operatore del Titolare
X	Le videocamere sono dotate di sistemi di antimanomissione
X	Le videocamere sono protette dall'azione degli agenti atmosferici
X	Le postazioni per il monitoraggio in tempo reale sono organizzate in modo da non consentire la visione dei monitor da parte di personale non autorizzato
X	Il sistema di registrazione delle immagini è distribuito (esistono più punti di raccolta) in zone diverse della struttura del Titolare
X	Il sistema di registrazione delle immagini è centralizzato presso la struttura del Titolare

MMS-ICT

Sono state adottate le **Misure Minime di Sicurezza ICT** per le Pubbliche Amministrazioni?

X	SI, il documento è allegato
	SI, il documento è in fase di predisposizione

	NO, è in corso la relativa valutazione
	NO

D. Esecuzione della Valutazione d'Impatto sulla Protezione dei Dati Personali (DPIA)

Il trattamento dei dati personali è un'attività che espone a rischio gli interessati, ossia le persone fisiche cui i dati si riferiscono.

I rischi per i diritti e le libertà delle persone fisiche possono derivare dal fatto che il trattamento, in ragione delle caratteristiche sue proprie, possa cagionare danni materiali e immateriali, come per esempio, discriminazioni, pregiudizio alla reputazione o qualsiasi altro danno economico o sociale significativo (**Considerando 75 del RGPD e Considerando 61 della Direttiva 2016/680**).

Posto che, sulla scorta delle considerazioni esposte nel paragrafo che precede, il trattamento in questione presenta "naturalmente" un rischio per i diritti e le libertà delle persone fisiche, la normativa di protezione richiede al Titolare del trattamento l'adozione di misure adeguate a gestire e limitare tale rischio.

Le attività di valutazione d'impatto sulla protezione dei dati personali (DPIA) sono finalizzate, prioritariamente, a contenere la probabilità e l'impatto che eventuali violazioni di dati personali (denominate nell'accezione inglese "data breach") potrebbero comportare sulle persone fisiche alle quali i dati si riferiscono.

Lo scopo è stabilire se e fino a che punto un'attività di trattamento, per le sue caratteristiche, il tipo di dati cui si riferisce o il tipo di operazioni svolte possa causare danni alle parti interessate e quali siano le misure disponibili per contenere il rischio (per esempio, la cifratura dei dati e la pseudonimizzazione, i test di sicurezza, i sistemi di continuità operative e le procedure di backup).

D.1. Analisi dei possibili impatti e loro gravità

Si cerca di determinare un reale e potenziale impatto sui diritti e le libertà degli interessati, **tenendo in considerazione i controlli e le contromisure esistenti**, pianificate o implementate al fine di ridurre tale rischio, utilizzando una scala di valori (basso, medio, alto, molto alto).

La valutazione tiene conto delle differenti ipotesi di danno (fisici, materiali o morali). A seconda delle circostanze, una violazione può riguardare tutti gli aspetti sottoindicati od una combinazione di essi.

Il livello di rischio può aumentare o diminuire considerando i seguenti fattori:
- natura, carattere sensibile e volume de dati personali trattati;
- livello di identificazione dei dati;
- natura della fonte del rischio;
- numero di interconnessioni (interessati, parti terze, stati esteri, …);
- numero e tipologia di dispositivi informatici impiegati.

Scala di misurazione dell'impatto (suggerita da ENISA)

LIVELLO DI IMPATTO	DESCRIZIONE
BASSO	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.)
MEDIO	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.)
ALTO	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.)
MOLTO ALTO	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

Le **minacce alla sicurezza** dei dati personali possono essere classificate, avendo riguardo al tipo di violazione dei dati personali che possono determinare, in:

violazione della riservatezza	in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali
violazione dell'integrità	in caso di modifica non autorizzata o accidentale dei dati personali
violazione della disponibilità	in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali

Questa scala di misurazione viene utilizzata per valutare, separatamente, l'impatto sulle persone fisiche derivante dalla violazione di riservatezza, integrità e disponibilità dei dati.

D.1.1. Perdita di riservatezza (Confidentiality Breach)

La perdita di confidenzialità o riservatezza consegue tipicamente a due violazioni: la divulgazione e l'accesso. Occorre determinare quale potrebbe essere l'impatto sull'Interessato nel caso in cui i dati raccolti dal sistema di videosorveglianza fossero oggetto di accesso ad opera di terzi non aventi diritto.

Con il termine "**divulgazione**" si intendono una comunicazione o diffusione non autorizzate od improprie dei dati personali, non corrispondenti ad informazioni di pubblico dominio, verso terze parti, anche se non note o identificabili. In alcuni casi la divulgazione può seguire un accesso ai dati da parte di soggetti non aventi diritto; in altri casi può essere dovuta a trattamenti non conformi di dati personali.

Con il termine "**accesso**" si intende l'accesso (anche in sola visualizzazione) ai dati trattati dal Titolare da parte di soggetti non aventi diritto al momento della violazione.
L'accesso ai dati non implica che si sia verificata anche un'altra violazione, quale la distruzione, l'alterazione o la divulgazione: il soggetto non avente diritto potrebbe utilizzare a proprio favore le informazioni ricavabili dai dati senza distruggerli, alterarli o divulgarli.

Occorre in ogni caso verificare se le misure di sicurezza (es.: cifratura dei dati) in uso rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note).
(Ad esempio, un documento cartaceo o un laptop contenente dati personali viene perso durante il trasporto; l'attrezzatura è stata smaltita senza distruzione dei dati personali; i dati personali vengono inviati erroneamente a una serie di destinatari non autorizzati; alcuni utenti potrebbero accedere agli account di altri utenti in un servizio online; i dati personali sono pubblicati su una bacheca Internet o su un sito p2p; un CD-ROM con i dati del cliente è stato rubato dai locali in cui era conservato, un sito web configurato in modo errato rende pubblicamente accessibili su internet i dati degli utenti interni).

Possibili conseguenze che una divulgazione non autorizzata (perdita di riservatezza) di dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato:

X	I dati potrebbero essere divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
X	I dati potrebbero essere oggetto di accesso da parte di soggetti non aventi diritto al momento della violazione
X	I dati potrebbero essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
X	I dati potrebbero essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito

Potenziale Impatto che una divulgazione non autorizzata (perdita di riservatezza) di dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato:

X	Perdita del controllo dei dati personali
X	Limitazione dei diritti
X	Discriminazione
N.A.	Furto o usurpazione di identità
N.A.	Frodi
N.A.	Perdite finanziarie
N.A.	Decifratura non autorizzata della pseudonimizzazione
X	Pregiudizio alla reputazione
X	Perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)
X	Conoscenza da parte di terzi non autorizzati
N.A.	Qualsiasi altro danno economico o sociale, significativo

Gravità dell'Impatto che una divulgazione non autorizzata (**perdita di riservatezza**) di dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato:

La gravità dell'impatto va considerata separatamente per le categorie di dati personali di cui agli articoli 9 e 10 del RGPD e, precisamente:

TIPOLOGIA DATO	GRAVITA' IMPATTO
DATI COMUNI	BASSO
DATI SENSIBILI (ART. 9 RGPD)	MEDIO
DATI GIUDIZIARI (ART. 10 RGPD)	ALTO

Nell'ambito delle operazioni di trattamento derivante dall'utilizzo di un sistema di videosorveglianza, l'impatto complessivo della perdita di riservatezza è da considerarsi considerato **MEDIO**, anche in considerazione del fatto che le informazioni raccolte dal sistema fanno riferimento a circostanze o condotte rese manifeste in un luogo pubblico o, comunque, aperto al pubblico.

D.1.2. Perdita di integrità (Integrity Breach)

Determinazione di quale potrebbe essere l'impatto sull'Interessato nel caso in cui i dati raccolti dal sistema di videosorveglianza fossero oggetto di un'**alterazione non autorizzata**.

La "alterazione" è la situazione in cui **i dati sono danneggiati, corrotti o non più completi**. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale).

L'alterazione non autorizzata dei dati può comportare:
- la comunicazione di informazioni erronee a soggetti esterni alla struttura del Titolare o al pubblico;
- errori nel trattamento o trattamento non conforme;
- decisioni errate con effetti sull'interessato.

In alcuni casi l'alterazione può seguire un accesso ai dati da parte di soggetti non aventi diritto; in altri casi può essere dovuta ad errori nel trattamento.

Occorre comunque verificare se sia possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.
(Ad esempio, è stato modificato un record necessario per la fornitura di un servizio sociale online e l'individuo deve richiedere il servizio in modalità offline; è stato modificato un record importante per l'accuratezza del file di un individuo in un servizio medico online).

Possibili conseguenze che un'alterazione non autorizzata (**perdita di integrità**) dei dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato

X	I dati potrebbero essere modificati e resi inconsistenti
X	I dati potrebbero essere modificati mantenendo la consistenza
X	Potrebbero essere comunicate informazioni erronee a soggetti esterni alla struttura del Titolare o al pubblico
X	Potrebbero esservi errori nel trattamento o verificarsi un trattamento non conforme
X	Potrebbero essere assunte decisioni errate con effetti sull'interessato

Potenziale Impatto che un'alterazione non autorizzata (**perdita di integrità**) di dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato

N.A.	Perdita del controllo dei dati personali
X	Limitazione dei diritti
N.A.	Discriminazione
X	Furto o usurpazione di identità
N.A.	Frodi
N.A.	Perdite finanziarie
N.A.	Decifratura non autorizzata della pseudonimizzazione
X	Pregiudizio alla reputazione
N.A.	Perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)
N.A.	Conoscenza da parte di terzi non autorizzati
X	Qualsiasi altro danno economico o sociale, significativo

Gravità dell'Impatto che un'alterazione non autorizzata (**perdita di integrità**) dei dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato:

La gravità dell'impatto va considerata separatamente per le categorie di dati personali di cui agli articoli 9 e 10 del RGPD e, precisamente:

TIPOLOGIA DATO	GRAVITA' IMPATTO
DATI COMUNI	BASSO
DATI SENSIBILI (ART. 9 RGPD)	MEDIO
DATI GIUDIZIARI (ART. 10 RGPD)	ALTO

Nell'ambito delle operazioni di trattamento derivante dall'utilizzo di un sistema di videosorveglianza, l'impatto complessivo della perdita di integrità è da considerarsi considerato **MEDIO**, anche in considerazione del fatto che le informazioni raccolte dal sistema fanno riferimento a circostanze o condotte rese manifeste in un luogo pubblico o, comunque, aperto al pubblico.

D.1.3. Perdita di disponibilità (Availability Breach)

Determinazione di quale potrebbe essere l'impatto sull'Interessato nel caso in cui i dati raccolti dal sistema di videosorveglianza fossero oggetto di una distruzione non autorizzata o perdita.

Con il termine "**indisponibilità**" si intende la indisponibilità, irreversibile o temporanea, dei mezzi e degli strumenti necessari per effettuare il trattamento dei dati da parte degli Interessati o del Titolare per l'erogazione di servizi richiesti o per conto dell'Interessato.
L'indisponibilità non implica la distruzione dei dati personali.
L'indisponibilità irreversibile di un mezzo o strumento, richiede l'adozione di nuovi mezzi o strumenti per accedere ai dati.
Tale violazione può essere relativa a:
- indisponibilità dei sistemi e dei servizi informatici mediante i quali le informazioni sono accessibili (ad es. in caso di attacco informatico);
- indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (ad es. perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi);
- indisponibilità degli strumenti atti ad identificare l'informazione all'interno di grandi archivi cartacei od elettronici;
- degrado prestazionale dei servizi informatici che determina l'impossibilità di perfezionare operazioni di trattamento;
- modifiche tecnologiche che rendono impossibile la decodifica dei dati rappresentati secondo particolari formati di memorizzazione.

Con il termine "**perdita**" si intende la perdita del supporto fisico di memorizzazione dei dati (ad es. privazione, sottrazione, smarrimento dei dispositivi contenenti i dati oppure dei documenti cartacei). La perdita di dati è la situazione in cui i dati, presumibilmente, esistono ancora, ma il Titolare ne ha perso il controllo o la possibilità di accedervi.
La perdita di un supporto fisico di memorizzazione dei dati non implica che si sia verificata anche un'altra violazione quale la distruzione, l'indisponibilità, l'accesso o la divulgazione (ad es., un disco DVD perso può contenere una copia cifrata dei dati).

Con il termine "**distruzione**" si intende la indisponibilità irreversibile o di lunga durata di dati personali trattati dal Titolare. La distruzione dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal Titolare.
La violazione può essere relativa a:
- eliminazione logica non autorizzata (ad es., cancellazione dei dati);
- eliminazione fisica (ad es., danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei);
- eliminazione logica o fisica dei dati in formato elettronico, il cui ripristino da documenti cartacei è possibile ma con un impiego di tempo elevato, tale da poter generare effetti sull'interessato.

In questo scenario, i dati personali possono essere recuperati solo:
* direttamente dall'Interessato;
* da fonti esterne quali fonti pubbliche e/o di terze parti;
* da archivi cartacei (in caso di distruzione, il recupero da tali archivi si suppone estremamente complesso, di lunga durata e con il rischio di ottenere dati non aggiornati).

Ci sarà sempre una violazione della Disponibilità del dato nel caso di perdita o distruzione permanente dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione.
(Ad esempio, un database di utenti è danneggiato ed è necessaria un'attività gravosa per riportare il servizio in linea; un file personale viene perso e l'individuo deve fornire nuovamente alcune informazioni all'Ente; un

file è stato perso/il database è danneggiato e non è stato eseguito il backup di queste informazioni; un servizio critico (ad es. cartella clinica online) è inattivo e non può essere recuperato immediatamente)

Possibili conseguenze che una distruzione non autorizzata (**perdita di disponibilità**) dei dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato

X	Mancato accesso a servizi
X	Malfunzionamento e difficoltà nell'utilizzo di servizi
N.A.	Impossibilità di decodifica dei dati rappresentati secondo particolari formati di memorizzazione
X	Mancato accesso alle informazioni

Potenziale Impatto che una distruzione non autorizzata (**perdita di disponibilità**) di dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato:

N.A.	Perdita del controllo dei dati personali
X	Limitazione dei diritti
N.A.	Discriminazione
N.A.	Furto o usurpazione di identità
N.A.	Frodi
X	Perdite finanziarie
N.A.	Decifratura non autorizzata della pseudonimizzazione
N.A.	Pregiudizio alla reputazione
N.A.	Perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)
N.A.	Conoscenza da parte di terzi non autorizzati
X	Qualsiasi altro danno economico o sociale, significativo

Gravità dell'Impatto che una distruzione non autorizzata o perdita (**perdita di disponibilità**) dei dati personali - raccolti dal sistema di videosorveglianza - potrebbe avere sull'Interessato.
La gravità dell'impatto va considerata separatamente per le categorie di dati personali di cui agli articoli 9 e 10 del RGPD e, precisamente:

TIPOLOGIA DATO	**GRAVITA' IMPATTO**
DATI COMUNI	BASSO
DATI SENSIBILI (ART. 9 RGPD)	MEDIO
DATI GIUDIZIARI (ART. 10 RGPD)	MEDIO

Nell'ambito delle operazioni di trattamento derivante dall'utilizzo di un sistema di videosorveglianza, l'impatto complessivo della perdita di disponibilità è da considerarsi considerato **MEDIO**, anche in considerazione del fatto che la tutela dei diritti dell'interessato può essere accompagnata da altri elementi di prova (prove documentali e testimoniali) essendo i fatti e le circostanze oggetto di ripresa, avvenuti in luogo pubblico od aperto al pubblico.

D.1.4. Impatto complessivo

Al termine delle valutazioni condotte, sono ottenuti tre diversi livelli di impatto (per la perdita di riservatezza, integrità e disponibilità).

Il più alto di questi livelli è considerato come il risultato finale della valutazione dell'impatto, relativo al trattamento complessivo dei dati personali.

La valutazione dell'impatto complessivo del trattamento mediante un sistema di videosorveglianza è:

	BASSO
X	**MEDIO**
	ALTO
	MOLTO ALTO

D.2. Analisi delle minacce e relativa probabilità di verificazione

Una minaccia è qualsiasi circostanza od evento che abbia il potenziale di influire negativamente sulla sicurezza dei dati personali.

In questa fase, l'obiettivo del Titolare del trattamento è comprendere le minacce relative all'ambiente generale del trattamento dei dati personali (esterno o interno) e valutarne la probabilità (probabilità di accadimento della minaccia).

Il rischio di un evento dannoso per i diritti degli interessati deriva dall'esposizione del dato a una o più minacce; quindi, identificare i rischi implica sempre considerare la minaccia che potrebbe originarli e anche le conseguenze che dalla stessa possono determinarsi.

Riprendendo la soprariportata classificazione dele minacce, avuto riguardo al tipo di violazione dei dati personali che possono determinare:

violazione della riservatezza	in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali
violazione dell'integrità	in caso di modifica non autorizzata o accidentale dei dati personali
violazione della disponibilità	in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali

E' possibile derivare i seguenti tre **scenari di rischio**:

accesso illegittimo	violazione della riservatezza
modifiche indesiderate	violazione dell'integrità
perdita dei dati	violazione della disponibilità

Analogamente a quanto fatto in relazione alla valutazione dell'impatto, la **valutazione della probabilità di accadimento** della minaccia può essere solo qualitativa, in quanto strettamente correlata allo specifico ambiente di trattamento dei dati personali.

La probabilità fa riferimento alla possibilità che il rischio si concretizzi.

Nell'ambito dell'approccio suggerito dall'ENISA, vengono definiti tre livelli di probabilità di occorrenza della minaccia, ovvero:

BASSO	è improbabile che la minaccia si materializzi
MEDIO	è possibile che la minaccia si materializzi
ALTO	è probabile che la minaccia si materializzi

Tradizionalmente si individuano le seguenti **tipologie di accadimento**, dalle quali si possono originare delle fonti di rischio.
Le fonti di rischio possono essere rappresentate da:
- persona, interna o esterna all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, ...);
- fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio. Può essere un incidente od un sinistro verificatosi presso uno dei soggetti incaricati del trattamento od anche presso Contitolari e Responsabili del trattamento

Possono costituire una "fonte di rischio umana interna" le seguenti situazioni:

- un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione.
- un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio.
Le motivazioni possono essere molteplici: confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.

Possono costituire una "fonte di rischio umana esterna" le seguenti situazioni:
- una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio;
- un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo;
- un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine;
- una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni.
Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

Fonti di rischio che possono coinvolgere il trattamento mediante sistema di videosorveglianza:

X	Azione intenzionale interna
X	Azione intenzionale esterna
X	Azione accidentale interna
X	Azione accidentale esterna

L'approccio suggerito dall'ENISA definisce **altresì quattro aree di valutazione** per la probabilità di insorgenza della minaccia e guida il controllore attraverso di esse, vale a dire:
- Risorse di rete e tecniche (hardware e software);
- Processi/procedure relative al trattamento dei dati personali;
- Soggetti coinvolti nel trattamento;
- Settore di attività e scala del trattamento.

D.2.1. Risorse di rete e tecniche (hardware e software)

	SI	NO
Una parte del trattamento dei dati personali viene eseguita tramite Internet?	X	
È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad es. per determinati utenti o gruppi di utenti)?	X	
Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno all'Ente?		X
Le persone non autorizzate possono accedere facilmente all'ambiente di elaborazione dei dati?		X
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le best practises in materia?		X

DETTAGLI: sebbene gli strumenti di lavoro utilizzati (server e client) dispongano di una connessione ad internet, essi sono sottoposti a misure di protezione quali firewall fisici e software, vpn, software anti-malware, istruzioni agli operatori, ecc.
L'interconnessione al sistema della Motorizzazione è garantita da idonee misure di sicurezza stabilite dal titolare della relativa piattaforma.

Valutazione di **probabilità**:

	BASSO (1)
X	MEDIO (2)
	ALTO (3)

D.2.2. Processi e procedure relativi all'operazione di trattamento dei dati personali

	SI	NO
I ruoli e le responsabilità in relazione al trattamento dei dati personali sono vaghi o non sono chiaramente definiti?		X
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non è chiaramente definito?		X
I dipendenti possono portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?		X
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti elaborare dati personali al di fuori dei locali dell'Ente?		X
Le attività di trattamento dei dati personali possono essere eseguite senza che vengano creati file di registro?		X

DETTAGLI: i soggetti autorizzati ad accedere al sistema di videosorveglianza ed effettuare operazioni di trattamento sono sottoposti ad adeguata formazione e puntuali istruzioni.

Valutazione di **probabilità**:

X	BASSO (1)
	MEDIO (2)
	ALTO (3)

D.2.3. Soggetti coinvolti nel trattamento dei dati personali

	SI	NO
Il trattamento dei dati personali è effettuato da un numero indefinito di dipendenti?		**X**
Una parte dell'operazione di elaborazione dei dati è svolta da un contraente/terza parte (responsabile del trattamento)?	**X**	
Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente indicati?		**X**
Il personale coinvolto nel trattamento dei dati personali non ha familiarità con le questioni di sicurezza?		**X**
I soggetti coinvolti nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali?		**X**

DETTAGLI: i soggetti autorizzati ad accedere al sistema di videosorveglianza ed effettuare operazioni di trattamento sono sottoposti ad adeguata formazione e puntuali istruzioni. Parimenti sono chiari i termini entro i quali i soggetti esterni possono eseguire operazioni di trattamento.

Valutazione di **probabilità**:

	BASSO (1)
X	MEDIO (2)
	ALTO (3)

D.2.4. Settore di operatività e scale di rilevanza del trattamento

	SI	NO
Ritieni che il settore di attività del Titolare sia soggetto ad attacchi informatici?	**X**	
Il Titolare del trattamento ha subito attacchi informatici o altri tipi di violazione della sicurezza negli ultimi due anni?		**X**
Il Titolare ha ricevuto nell'ultimo anno segnalazioni e/o reclami in merito alla sicurezza del sistema informatico (utilizzato per il trattamento dei dati personali)?		**X**
Le operazioni di trattamento riguardano un grande volume di persone e/o dati personali?	**X**	
Esistono best practices o disposizioni normative di sicurezza specifiche, per il settore di attività del Titolare del trattamento, che non sono state adeguatamente seguite?		**X**

DETTAGLI: il settore delle pubbliche amministrazioni è recentemente risultato essere vittima di attacchi informatici da parte di malintenzionati. Tuttavia, questo Titolare del trattamento non ha subito violazioni di sicurezza con riferimento al sistema di videosorveglianza che risulta adeguatamente protetto attraverso l'adozione delle misure tecniche ed organizzative descritte in precedenza.

Valutazione di **probabilità**:

	BASSO (1)
X	MEDIO (2)
	ALTO (3)

D.2.5. Valutazione della probabilità di occorrenza delle minacce

La **probabilità di occorrenza finale** della minaccia viene calcolata dopo aver sommato i diversi punteggi ottenuti in relazione a ciascuna area.

Il risultato della somma determinerà il livello complessivo di probabilità di verificazione delle minacce sulla scorta della tabella che segue.

Somma globale della probabilità di occorrenza di una minaccia	**Livello di probabilità delle minacce**
4-5	BASSO
6-8	MEDIO
9-12	ALTO

Valore numerico della probabilità complessiva (dato dalla sommatoria dei punteggi attribuiti nei precedenti paragrafi:

PARAGRAFO	**PROBABILITÀ**	**VALORE**
D.2.1	MEDIO	2
D.2.2	BASSO	1
D.2.3	MEDIO	2
D.2.4	MEDIO	2
TOTALE	**MEDIO**	**7**

Livello globale di probabilità delle minacce: MEDIA

D.3. Valutazioni e Piano di trattamento dei rischi

Considerato che:
- a norma dell'**articolo 35, paragrafo 9, del RGPD** "*Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti*";
- a norma dell'**articolo 36, paragrafo 1, del RGPD** "*Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*";

Con particolare riferimento alla c.d. **consultazione preventiva** di cui all'art. 36 del RGPD, si recepiscono le indicazioni contenute nelle Linee Guida rilasciate dal Gruppo di lavoro articolo 29 per la protezione dei dati, come modificate e adottate da ultimo il 4 ottobre 2017 (**WP 248 rev.01**), a tenore delle quali "*Ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo*".
"*Inoltre, il titolare del trattamento dovrà consultare l'autorità di vigilanza qualora il diritto dello Stato membro in questione prescriva che i titolari del trattamento consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, paragrafo 5)*"

Ritenuta la non necessità di procedere ad acquisire il parere degli interessati, trattandosi di un trattamento necessario per l'esecuzione di un compito di interesse pubblico ovvero svolto nel contesto della prevenzione e repressione dei reati.

Acquisito il parere del Responsabile della Protezione dei Dati Personali (RPD)

Alla luce delle informazioni raccolte e dei risultati della presente valutazione di impatto, **SI RITIENE**:

N.A.	possibile procedere con l'implementazione del progetto e l'avvio del trattamento senza ulteriori misure tecniche e organizzative
X	possibile procedere con l'implementazione del progetto e l'avvio del trattamento senza ulteriori misure tecniche e organizzative, ma si suggerisce di implementare le misure tecniche e organizzative specificamente indicate
N.A.	possibile procedere con l'implementazione del progetto e l'avvio del trattamento, solo dopo aver implementato le misure tecniche e organizzative ulteriori specificamente indicate
N.A.	necessario/opportuno raccogliere le opinioni degli interessati o dei loro rappresentanti, in merito al trattamento
N.A.	necessario consultare l'Autorità di controllo prima di iniziare il trattamento

D.4. Formalizzazione dei risultati, revisione ed aggiornamento

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, concorre alla realizzazione del presente report finale, in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dalla normativa di protezione dei dati personali.

Il report deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

La presente DPIA sarà sottoposta a revisione ed aggiornamento, qualora ciò si rendesse necessario a seguito della modifica di taluno dei suoi elementi costitutivi. In ogni caso, sarà oggetto di nuova valutazione con cadenza annuale.

L'attività di revisione ed aggiornamento è condotta dal soggetto designato dal Titolare del trattamento, il quale vi provvede coinvolgendo il Responsabile della Protezione dei Dati Personali (DPO).