Regolamento
del sistema di videosorveglianza
per la sicurezza cittadina

Sommario

Regolamento del sistema di videosorveglianza per la sicurezza cittadina

CAPO I - DISPOSIZIONI GENERALI

Art. 1 – Oggetto

1. Il presente Regolamento, comprensivo degli allegati, disciplina il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza attivati nel territorio del Comune e garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

2. Il presente regolamento:
   2.1. definisce le modalità di utilizzo degli impianti di videosorveglianza;
   2.2. disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza.

3. Gli impianti di videosorveglianza attivati nel Comune:
   3.1. riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese;
   3.2. le videocamere consentono riprese video anche a colori e audio come da schema in **Allegato 1**

4. Sono attivabili impianti di foto sorveglianza e videosorveglianza mobili, posizionabili in aree del territorio comunale individuate dal Comando Unico di Polizia Locale, oppure montate su veicoli di servizio e utilizzabili per le finalità, quelle applicabili, indicate nell'art. 4 del presente regolamento.

5. Sono in uso dispositivi per la rilevazione di immagini e video mobili "Body Cam", utilizzabili per le finalità, quelle applicabili, indicate nell'art. 4 del presente regolamento.

6. Sono attivabili sistemi di videosorveglianza su droni utilizzabili per le finalità, quelle applicabili, indicate nell'art. 4 del presente regolamento e utilizzabili soltanto dai soggetti individuati dal Titolare e in possesso dei requisiti tecnici e delle autorizzazioni ufficiali per poter pilotare il mezz**o.**
   Tale attività deve essere svolta solo a seguito di istruzione motivata e documentata. L'uso dei droni deve essere sempre rispettoso dei principi ispiratori della normativa sulla tutela e la protezione delle persone fisiche in relazione al Trattamento dei dati personali, in particolare seguendo le indicazioni dell'Autorità Garante in merito

7. L'utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada è soggetto a questo regolamento ove, le disposizioni, non siano in contrasto con particolari provvedimenti del Garante per la protezione dei dati nonché dalla specifica normativa di settore.

Art. 2 - Norme di riferimento e principi generali

1. Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto dal:
   - Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito RGPD) 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"
   - Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio" recepita dal D.lgs. 51/2018.
   - Legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Municipale

- Legge 20 maggio 1970, n. 300, “Statuto dei lavoratori”
- Legge 241/90 “Legge sul procedimento amministrativo”
- Decreto Legislativo 267/2000, “T.U. Enti locali”
- Decreto-legge 23 febbraio 2009, n. 11 "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonchè in tema di atti persecutori" pubblicato nella *Gazzetta Ufficiale* n. 45 del 24 febbraio 2009
- Legge 18 aprile 2017, n. 48, recante “Disposizioni urgenti in materia di sicurezza delle città” (già Decreto Legge 20 febbraio 2017, n. 14)
- Decreto Legislativo 196/2003 ss.mm.ii. “Codice Privacy” come aggiornato al D.lgs. 101/2018
- DPR n. 15 del 15/01/2018 recante “Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196 ss.mm.ii. recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia”
- Legge regionale n. 6/2015, dallo statuto e dai regolamenti comunali
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell’8 aprile 2010 (G.U. n. 99 del 29/04/2010)
- Convenzione tra i Comuni coinvolti per l’area di Polizia Locale

2. La Videosorveglianza in ambito comunale si fonda sui principi applicabili al trattamento di dati personali di cui all’art. 5, RGDP e, in particolare:
   - Principio di liceità – Il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando 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 in ossequio al disposto di cui all’art. 6, Paragrafo 1, lett. e), RGPD. La videosorveglianza comunale, pertanto, è consentita senza necessità di consenso da parte degli interessati.
   - Principio di necessità – In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all’art. 5, Paragrafo 1, lett. c), RGPD, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l’utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l’interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.
   - Principio di proporzionalità
   - La raccolta e l’uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un’effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento. Nell’uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l’angolo di visuale all’area effettivamente da proteggere.
   - Principio di finalità – Ai sensi dell’art. 5, Paragrafo 1, lett. b), RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia

incompatibile con tali finalità. È consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana.

Art. 3 – Definizioni

1. Ai fini del presente regolamento si intende per:
   1.1. “dato personale”: qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

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

   1.3. “profilazione”: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

   1.4. “pseudonimizzazione”: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

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

   1.6. “responsabile del trattamento”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

   1.7. “incaricato del trattamento”: la persona fisica che abbia accesso a dati personali.

   1.8. “interessato”, la persona fisica identificata o identificabile cui si riferiscono i dati personali oggetto di trattamento.

   1.9. “terzo”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate a trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

   1.10. “violazione dei dati personali”: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

1.11. “comunicazione”: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.12. “diffusione”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.13. “dato anonimo”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

1.14. “Sicurezza Urbana”: il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione, anche urbanistica, sociale e culturale, e recupero delle aree o dei siti degradati , l’eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, la promozione della cultura del rispetto della legalità e l’affermazione di più elevati livelli di coesione sociale e convivenza civile.

Art. 4 – Finalità

1. Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conformi alle funzioni istituzionali demandate al Comando Unico di Polizia Locale dalla normativa già citata e dalle altre disposizioni normative applicabili al Comune.
   In particolare, l’uso di impianti di videosorveglianza è strumento per l’attuazione di un sistema integrato di politiche per la sicurezza urbana, di cui alle fonti normative sopra citate.

2. L’utilizzo degli impianti di videosorveglianza è finalizzato a:
   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” e delle attribuzioni del Sindaco in qualità di autorità locale di cui all’art. 50 e di ufficiale di governo di cui all’art. 54 comma 4 e 4-bis del D.lgs. 267/2000;
   b) 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;
   c) vigilare sull’integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
   d) tutelare l’ordine, il decoro e la quiete pubblica;
   e) controllare aree specifiche del territorio comunale;
   f) monitorare i flussi di traffico;
   g) verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici;
   h) attivare uno strumento operativo di protezione civile sul territorio comunale.

3. Il sistema di videosorveglianza in uso presso il Comando Unico di Polizia Locale è di tipo “integrato”, consentirebbe con i giusti accorgimenti, l’utilizzo condiviso eventualmente con altre Forze dell’Ordine presenti sul territorio comunale, quale strumento di prevenzione e di razionalizzazione dell’azione di polizia su tutto il territorio.

4. La possibilità di avere in tempo reale dati e immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell’ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

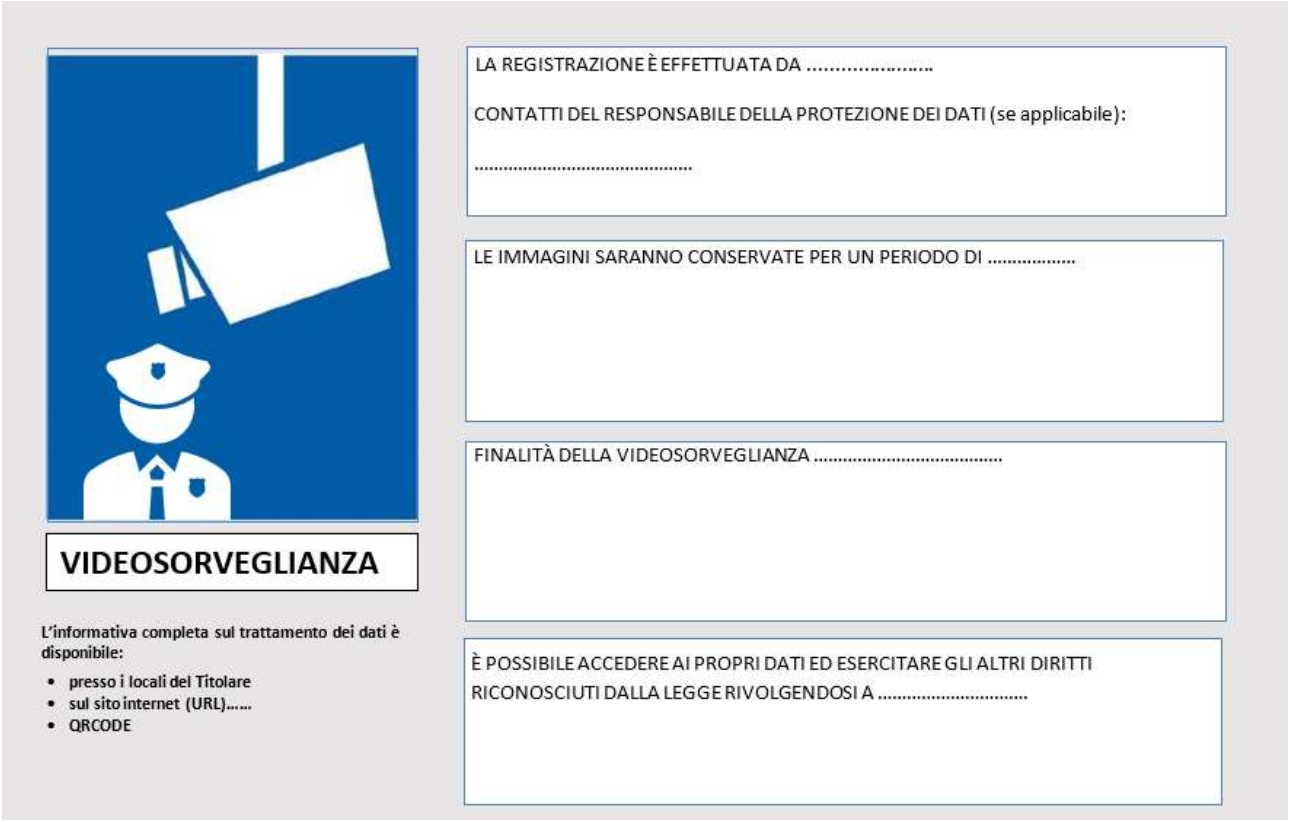
5. Ai sensi di quanto previsto dalla normativa gli impianti di videosorveglianza non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

6. Gli impianti di videosorveglianza non possono essere utilizzati per l'irrogazione di sanzioni per infrazioni del Codice della strada, se non omologate ai sensi dell'art. 201 del CdS.

Art. 5 – Informativa

1. Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici.

2. A tal fine l'Ente utilizzerà, adeguatamente compilato vd. **Allegato 2**, il modello grafico fornito come suggerimento da EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020 seguito richiamato:



3. L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere prima del raggio di azione delle telecamere.

4. La segnaletica deve essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.

5. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.

6. L'Ente si obbliga a rendere pubblici, tramite il sito internet e/o mezzi di diffusione locale di altro tipo eventuali variazioni in merito al sistema di videosorveglianza che possano avere un impatto sulla cittadinanza.

7. L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

8. Nel caso in cui la disposizione dei cartelli informativi sia sproporzionata alle finalità del trattamento dovuto ad un controllo di una zona di ampia dimensione, si provvederà ad informare i soggetti interessati tramite apposita diffusione sul sito istituzionale della zona soggetta al trattamento.

Art. 6 - Valutazione di Impatto sulla protezione dei dati

1. In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), RGPD, qualora il trattamento di dati realizzato mediante il sistema di videosorveglianza comunale dia luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, l'Ente procederà ad una valutazione di impatto sulla protezione dei dati personali che verrà allegata al presente regolamento e sarà messa a disposizione dell'Autorità su richiesta.

2. Parimenti si procederà nei casi in cui, il trattamento di dati realizzato mediante il sistema di videosorveglianza presenti un rischio comunque elevato per i diritti e le libertà delle persone fisiche.

CAPO II- SOGGETTI

Art. 7 – Titolare

1. Il Comune, insieme ad altri Enti secondo gli accordi vigenti, è titolare del trattamento dei dati personali acquisiti mediante utilizzo degli impianti di videosorveglianza di cui al presente regolamento. A tal fine il Comune è rappresentato, pro tempore, dal Sindaco, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.

2. Il Sindaco, in qualità di rappresentante del titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza:
a) definisce le linee organizzative per l'applicazione della normativa di settore;
b) effettua le notificazioni al Garante per la protezione dei dati personali;
c) nomina i responsabili dei dati trattati acquisiti mediante l'utilizzo degli impianti di videosorveglianza impartendo istruzioni ed assegnando compiti e responsabilità;
d) detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;
e) vigila sulla puntuale osservanza delle disposizioni impartite.

Art. 8 – Designato al trattamento dei dati trattati (Allegato 6)

1. Il Comandante del Comando Unico di Polizia Locale, individuato in concerto dai Sindaci, è il designato per la gestione dei dati personali trattati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento. La nomina è effettuata con atto del Sindaco, nel quale sono analiticamente specificati i compiti affidato al responsabile, in particolare:

- il Responsabile del trattamento, informato il Sindaco, individuerà e nominerà con propri atti i soggetti autorizzati al trattamento e l'utilizzo degli impianti di videosorveglianza, impartendo loro apposite istruzioni organizzative e operative scritte per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, RGPD; detti soggetti saranno opportunamente istruiti e formati da parte del Responsabile del trattamento con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;
- il Responsabile provvede a rendere l'informativa "minima" agli interessati secondo quanto definito nel presente regolamento (**Allegato 2**);

- il Responsabile verifica e controlla che il trattamento dei dati effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui all'art. 5 del RGPD e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;
- il Responsabile assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- il Responsabile, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;
- il Responsabile assiste il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;
- il Responsabile assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;
- il Responsabile garantisce l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;
- il Responsabile assicura l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;
- il Responsabile assiste il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;
- il Responsabile assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e nelle successive eventuali attività conseguenti;
- il Responsabile affianca il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico; **(Allegato 8)**
- il Responsabile garantisce che il Responsabile della Protezione dei Dati designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;
- il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;
- il Responsabile è responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- il Responsabile assicura che i soggetti autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
- il Responsabile garantisce la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale autorizzato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;

- il Responsabile vigila sul rispetto da parte dei soggetti autorizzati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Art. 9 – Soggetti autorizzati al trattamento dei dati personali (Allegato 6)

1. Il Comandante del Comando Unico di Polizia Locale o i diversi soggetti individuati dal Sindaco autorizzano dei soggetti in numero sufficiente a garantire il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento.
   L'autorizzazione è effettuata con atto scritto, nel quale sono analiticamente specificati i compiti affidati ai soggetti autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati. I soggetti autorizzati sono designati tra gli appartenenti al Comando Unico di Polizia Locale che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

2. In particolare, i soggetti autorizzati devono:
   - per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
   - conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
   - mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
   - custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
   - evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile dei dati trattati;
   - mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
   - conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
   - fornire al Responsabile dei dati trattati ed al Responsabile della Protezione dei dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

3. Tra i soggetti autorizzati al trattamento verranno individuati, con l'atto di nomina, le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti magnetici.

4. I soggetti autorizzati devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del Responsabile.

5. L'utilizzo degli apparecchi di ripresa da parte dei soggetti autorizzati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.

6. eventuali soggetti che svolgono fra il personale dell'ente mansioni di amministratore di sistema verranno appositamente designati da soggetti aventi titolo di rappresentare negli specifici contesti il titolare del trattamento.

Art. 10 - Soggetti esterni (Allegato 6)

1. Il Responsabile dei dati trattati, che svolge mansioni di coordinamento nell'ambito del trattamento dei dati, è autorizzato a ricorrere a Responsabili esterni del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato, in tutti i casi in cui egli, per la gestione/assistenza del sistema di videosorveglianza,

faccia ricorso a soggetti esterni ai quali affidare incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente.

2. In questi casi, il Responsabile dei dati trattati procederà a disciplinare i trattamenti da parte del responsabile esterno mediante contratto ovvero altro atto giuridico che vincoli il Responsabile esterno del trattamento al Titolare del trattamento ai sensi dell'artt. 28 e 29, RGPD. Qualora tra le mansioni del Responsabile esterno rientrino anche compiti relativi all'amministrazione di sistemi informatici, la designazione prevedrà anche gli aspetti di competenza in ottemperanza alle prescrizioni in materia di amministratore di sistema.

3. La visione e l'estrazione delle immagini da parte delle Forze dell'Ordine può essere realizzata mediante richiesta scritta e successivo ritiro del supporto digitale (fornito dall'istante), contenente le videoregistrazioni richieste, presso il Comando di Polizia Locale. In luogo della richiesta di cui al comma precedente, ai sensi e per gli effetti delle disposizioni vigenti, le Forze dell'Ordine possono acquisire direttamente la registrazione delle immagini conservate presso il Comando di Polizia Locale, nel qual caso è redatto apposito verbale di acquisizione. .

CAPO III - TRATTAMENTO DEI DATI PERSONALI

Art. 11 - Modalità di raccolta, trattamento e conservazione dei dati

1. L'installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili) in conformità all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale ai sensi del successivo art. 21.

2. L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle riprese evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.

3. Il titolare del trattamento dei dati personali si obbliga a non trasmettere a soggetti terzi riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità perseguite dalle registrazioni svolte dall'impianto attivato.

4. I segnali video delle unità di ripresa sono inviati presso la sede del Comando Unico di Polizia Locale o data center individuato appositamente dove sono registrati su appositi server. Il segnale è successivamente rilanciato alle centrali operative del Comando Unico di Polizia Locale, (alle Forze dell'ordine nel caso di collegamento) a ciò autorizzate. In queste sedi le immagini sono visualizzate su monitor e hardware client appositamente configurato. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, ai fini del soddisfacimento delle finalità di cui all'articolo 4 del presente regolamento.

5. I dati personali oggetto di trattamento sono:
   - trattati in modo lecito e secondo correttezza;
   - raccolti e registrati per le finalità di cui al presente regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;
   - raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

6. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione (secondo l'art. 6, co. 8, del D.L. 23/02/2009, n. 11 nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana).

Le registrazioni delle videocamere che rientrano nella disciplina dello Statuto dei Lavoratori adeguano il periodo di Data Retention alle disposizioni normative (24-72 ore).

7. In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Responsabile potrà disporre la conservazione delle immagini per un periodo di tempo superiore allo standard nel rispetto della normativa di settore e delle indicazioni/necessità dell'autorità giudiziaria.

8. Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato così da realizzare l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, mediante sovrascrittura, con modalità tali da rendere non riutilizzabili i dati cancellati.

9. Viene adottata politica per la cancellazione dei dati così da impedirne il recupero sia in fase di operatività ordinaria che in relazione allo smaltimento dei dispositivi elettrici ed elettronici.

Art. 12 - Diritti dell'interessato

1. In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, su presentazione di apposita istanza, ha diritto:
   a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
   b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
   c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.

2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sulla home page del sito istituzionale dell'Ente alla Sezione "Privacy") ovvero al Responsabile del trattamento dei dati individuato nel Comandante della Polizia Locale.

3. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
   - il luogo, la data e la fascia oraria della possibile ripresa;
   - l'abbigliamento indossato al momento della possibile ripresa;
   - gli eventuali accessori in uso al momento della possibile ripresa;
   - l'eventuale presenza di accompagnatori al momento della possibile ripresa;
   - l'eventuale attività svolta al momento della possibile ripresa;
   - eventuali ulteriori elementi utili all'identificazione dell'interessato.

4. Il responsabile della protezione dei dati dell'Ente ovvero il Responsabile del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.

5. Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei file contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche

eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.

6. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

7. Nell'esercizio dei diritti l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.

8. Le informazioni da fornire agli interessati nel rispetto degli artt. 12,13 e 14 RGPD saranno fornite in primo luogo tramite l'informativa "minima" e le informative estese saranno disponibili presso i locali dell'Ente e pubblicate sul sito istituzionale dell'Ente. .

CAPO IV- MISURE DI SICUREZZA

Art. 13 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del presente regolamento.

2. I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio.
   Dette misure, in particolare, assicurano:
   a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
   c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distribuzione, perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.

4. A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:
   a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti designati quali responsabili e incaricati del trattamento, dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le operazioni di competenza;
   b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate di effettuare sulle medesime immagini operazioni di cancellazione o di duplicazione;
   c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
   d) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le

necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;

e) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie Wi–Fi, Wi Max, Gprs).

5. Come già indicato, il titolare procede a designare con atto scritto il Responsabile dei dati trattati e, quest'ultimo provvede ad individuare, sempre in forma scritta, le persone fisiche autorizzate al trattamento, autorizzate ad accedere ai locali dove sono situate le postazioni di controllo, ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

6. Il Titolare ed il Responsabile dei dati trattati vigilano sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvedono altresì ad istruire e formare i soggetti autorizzati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

Art. 14 - Accesso alle centrali di controllo

1. I dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono custoditi presso il data center e le centrali di controllo ubicate presso il Comando Unico di Polizia Locale, nonché presso le altre sedi (Comune di Mesero) collegate;

2. L'accesso alle centrali di controllo è consentito esclusivamente al titolare, ai responsabili e ai soggetti autorizzati, individuati ai sensi del presente regolamento e indicati negli allegati.

3. L'accesso da parte di soggetti diversi da quelli indicati è subordinato al rilascio, da parte del titolare o dei responsabili, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. L'accesso avviene in presenza di soggetti autorizzati del Comando Unico di Polizia Locale individuati ai sensi del presente regolamento.

4. Fermo quanto già previsto, l'accesso alle centrali di controllo può essere consentito esclusivamente ad incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità del trattamento, nonché al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali.

5. I responsabili impartiscono idonee istruzioni atte ad evitare assunzioni o rilevamenti di dati da parte dei soggetti autorizzati all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali garantendo la riservatezza delle informazioni.

6. Gli incaricati vigilano sul puntuale rispetto delle istruzioni impartite dai responsabili e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 15 - Accesso agli impianti e ai dati

1. L'accesso agli impianti di videosorveglianza di cui al presente regolamento avviene da postazioni dedicate situate all'interno della sede del Comando Unico di Polizia Locale, o di altre Forze dell'Ordine in caso di collegamento, a ciò autorizzate, dal momento in cui ci fosse un collegamento, di registrazione remote qualora non sia tecnicamente possibile la trasmissione dati alla centrale operativa del Comando P.L. L'accesso ai dati può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate dal responsabile del trattamento.

2. L’accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità indicate nel presente regolamento e nel rispetto della norma di legge.

3. 3.L’accesso alle immagini è consentito esclusivamente:
   a) al Titolare, al Responsabile ed agli autorizzati del trattamento;
   b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall’Ente) nonché per finalità di indagine dell’Autorità Giudiziaria (sulla base di formale richiesta proveniente dall’A.G. e acquisita dall’Ente);
   c) alla società fornitrice dell’impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell’impianto medesimo ovvero, in casi del tutto eccezionali, all’amministratore informatico del sistema comunale (preventivamente individuato quale incaricato del trattamento dei dati);
   d) all’interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta. L’accesso da parte dell’interessato sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l’accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte del responsabile del trattamento, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;
   e) ai soggetti legittimati all’accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all’art. 24, comma 7, L. 241/90, l’accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente.

CAPO V- TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 16 – Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

1. Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e s.s., RGPD ed alle disposizioni attuative.

Art. 17 - Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali

1. Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all’art. 82, RGPD.

2. Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l’evento dannoso non gli è in alcun modo imputabile.

3. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2, RGPD.

CAPO VI - DISPOSIZIONI FINALI

Art. 18 – Provvedimenti attuativi

1. Compete alla Giunta Comunale l’assunzione dei provvedimenti attuativi conseguenti al presente Regolamento, in particolare la predisposizione dell’elenco dei siti di ripresa, la fissazione degli orari delle registrazioni, nonché la definizione di ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento.

Art. 19 – Entrata in vigore

1. Il presente regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.

2. Gli allegati potranno essere soggetti ad aggiornamento senza delibera di approvazione ma verranno notificati all'organo competente per validazione e conferma di recepimento dell'aggiornamento.

3. Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.

ALLEGATI:

1. Inventory - censimento posizione e tipologia telecamere
2. Cartello videosorveglianza [art. 13 RGPD]
3. Informativa estesa [art. 13 RGPD]
4. Misure tecniche e organizzative [artt. 24, 25, 32 RGPD]
5. Procedura per l'accesso alle immagini ed esercizio dei diritti [artt. 15, 17, 18, 19, 20, 21 RGPD]
   5.1. Formulario per esercizio di diritti [artt. 15, 17, 18, 19, 20, 21 RGPD]
6. Soggetti autorizzati al trattamento dei dati personali [artt. 28, 29]
7. Registro degli accessi [art. 29 RGPD]
8. Pagina di Registro delle attività di trattamento [art. 30 RGPD]

Allegato 1: Inventory - censimento posizione e tipologia telecamere

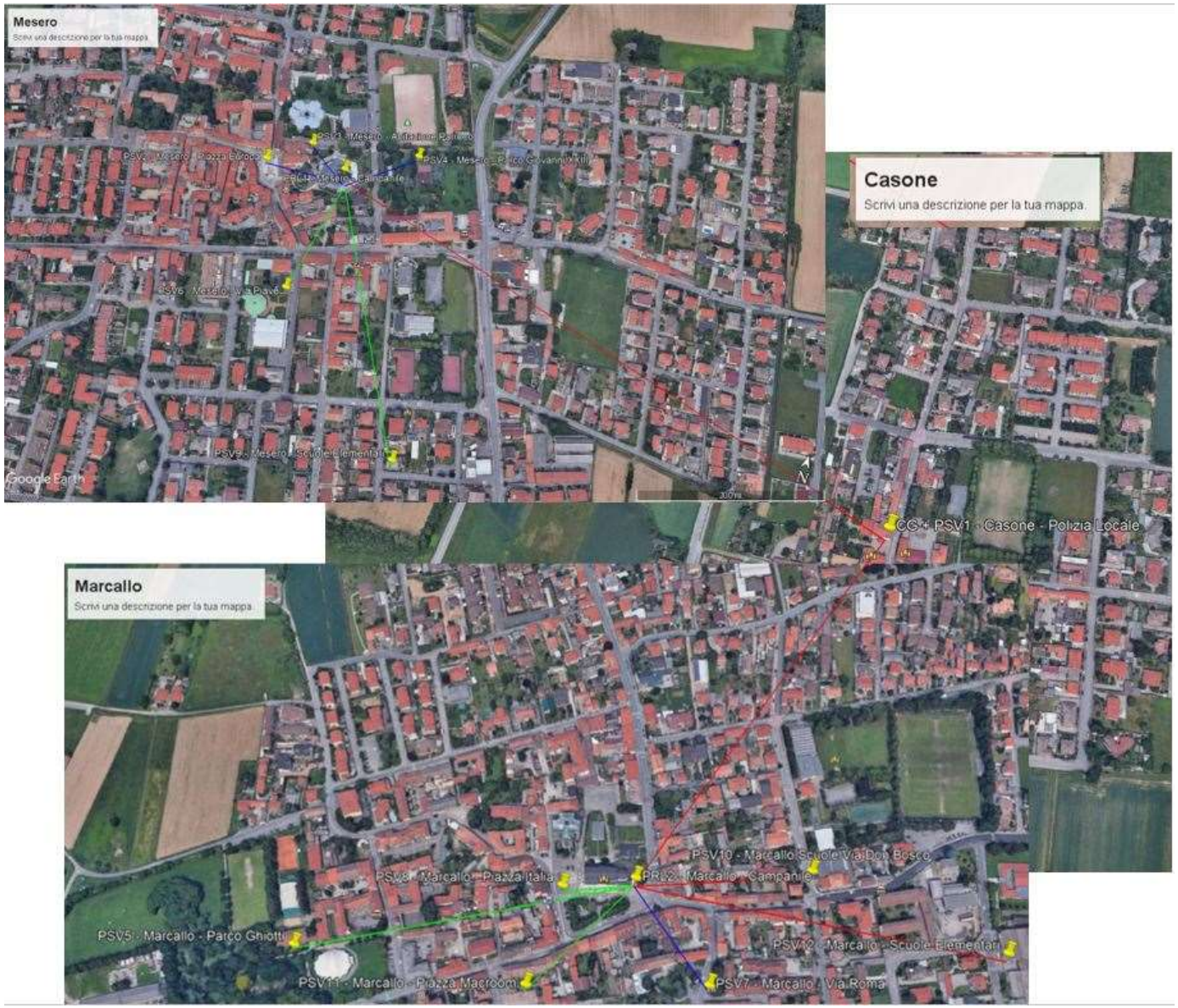
Comune in cui sono presenti	TELECAMERA	QUANTITÀ	AUDIO	RICONOSCIMENTO AUTOMATICO	COLORE	REGISTRAZIONE (e cancellazione)	VALUTAZIONE DELL'USO DELLE ATTREZZATURE (MOTIVAZIONI)
MARCALLO/ MESERO	macchine	1	no	sì	Sì	7 giorni (sovrascrittura automatica)	L'aspettativa di privacy in un centro città è molto bassa; i nostri centri cittadini sono ben segnalati con segnaletica adeguata per l'uso e lo scopo della videosorveglianza con i dettagli di contatto.
	fototrappole	x	Sì/no	Sì/no	Sì	manuale	
Casone Polizia Locale	TLC IP	3	NO	NO	Sì	7 giorni (sovrascrittura automatica)	
Marcallo Via Roma	TLC IP	2	NO	NO	Sì	7 giorni (sovrascrittura automatica)	
Marcallo Parco Ghiotti	TLC IP	5	NO	NO	Sì	7 giorni (sovrascrittura automatica)	
Marcallo Piazza	TLC IP	2	NO	NO	Sì	7 giorni (sovrascrittura automatica)	

Macroom							
Marcallo Scuole Via Don Bosco	MULTIOTTICA	1 (4 ottiche)	NO	NO	Sì	7 giorni (sovrascrittura automatica)	
Marcallo Piazza Italia	• TLC IP	5	NO	NO	Sì	7 giorni (sovrascrittura automatica)	
Marcallo Scuole Elementari Via al Donatore di Sangue	• TLC IP • MULTIOTTICA	1 1 (4 ottiche)	NO	NO	Sì	7 giorni (sovrascrittura automatica)	
Mesero Scuole Elementari Via Papa Pio XII	TLC IP	2	NO	In ATTESA DELL'AUTORIZZAZIONE PER LETTURA TARGHE (PREVISTA IMPLEMENTAZIONE OTTOBRE 2021)	Sì	7 giorni (sovrascrittura automatica)	
MESERO	Varchi (solo su mesero e non per marcallo)	x	Sì/no		Sì	7 giorni (sovrascrittura automatica)	
Mesero Piazza Europa	TLC IP	1	NO	In ATTESA DELL'AUTORIZZAZIONE PER LETTURA TARGHE (PREVISTA IMPLEMENTAZIONE OTTOBRE 2021)	Sì	7 giorni (sovrascrittura automatica)	
Mesero Piazza Europa (Abitazione Parroco)	TLC IP	1	NO	In ATTESA DELL'AUTORIZZAZIONE PER LETTURA TARGHE (PREVISTA IMPLEMENTAZIONE OTTOBRE 2021)	Sì	7 giorni (sovrascrittura automatica)	

Mesero Parco Via Giovanni XXIII	TLC IP	1	NO	In ATTESA DELL'AUTORIZZAZIONE PER LETTURA TARGHE (PREVISTA IMPLEMENTAZIONE OTTOBRE 2021)	Sì	7 giorni (sovrascrittura automatica)	
Mesero Via Piave	TLC IP	3	NO	In ATTESA DELL'AUTORIZZAZIONE PER LETTURA TARGHE (PREVISTA IMPLEMENTAZIONE OTTOBRE 2021)	Sì/no	7 giorni (sovrascrittura automatica)	
BODYCAM		2		NO		Manuale vd. Procedura operativa	
DRONI		N/a		NO		Manuale vd. Procedura operativa	
CAR-CAM		1		NO		Manuale vd. Procedura operativa	

Numero totale delle Telecamere: **26 TLC IP + 2 Multi Ottiche (4 Ottiche)**.

OCR = Telecamere Lettura Targhe
TLC = Telecamera di Contesto


Mesero
Scrivi una descrizione per la tua mappa
PSV4 - Mesero - Parco Giovanni XXIII
PSV6 - Mesero - Via Piave
PSV3 - Mesero - Scuole Elementari
Google Earth
Casone
Scrivi una descrizione per la tua mappa
CC + PSV1 - Casone - Polizia Locale
Marcallo
Scrivi una descrizione per la tua mappa
PSV10 - Marcallo Scuole Via Don Bosco
PSV8 - Marcallo - Piazza Italia
PR+2 - Marcallo - Campanile
PSV5 - Marcallo - Parco Ghiotti
PSV12 - Marcallo - Scuole Elementari
PSV11 - Marcallo - Piazza Macrom
PSV7 - Marcallo - Via Roma

Allegato 2: Cartello videosorveglianza

L'informativa completa sul trattamento dei dati è disponibile:

- **presso i locali della Polizia Locale**
- **sul sito internet dei Comuni sezione Privacy o Informative trattamento dati personali**
- **richiesta tramite email all'indirizzo privacy@marcallo.it**

CONTITOLARI: LA REGISTRAZIONE È EFFETTUATA DAI COMUNI DI MARCALLO CON CASONE E MESERO TRAMITE IL COMANDO UNICO DI POLIZIA LOCALE.

PERIODO DI CONSERVAZIONE: 7 giorni

FINALITÀ:

a) prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità
b) garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana"
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
d) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato
e) tutelare l'ordine, il decoro e la quiete pubblica
f) monitorare i flussi di traffico
g) verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici

DIRITTI DEGLI INTERESSATI: È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI

→ AL COMANDO DI POLIZIA IN Via S. Jacini, n° 145 - Marcallo con Casone OPPURE TRAMITE MAIL ALL'INDIRIZZO : polizialocale@marcallo.it

→ AL RESPONSABILE DELLA PROTEZIONE DEI DATI VIA MAIL ALL'INDIRIZZO: rpd@marcallo.it

Allegato 3: Informativa estesa

INFORMATIVA VIDEOSORVEGLIANZA

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI DEL COMUNE DI MESERO e di MARCALLO CON CASONE
SUL TRATTAMENTO DI VIDEOSORVEGLIANZA

INTRODUZIONE:
Il Comune tratta dati personali per lo svolgimento della propria attività istituzionale e per fornire assistenza e supporto alla cittadinanza.
La presente informativa, resa ai sensi della normativa europea e del "Codice Privacy", riporta le informazioni che l'interessato deve conoscere riguardo al trattamento dei propri dati personali relativamente alla videosorveglianza su suolo pubblico.

CONTITOLARE

Contitolare del trattamento
Il Comune di Mesero rappresentato pro tempore dal Sindaco.
Indirizzo: Via San Bernardo 41 - 20010 Mesero (MI)
e-mail:
SEGRETERIA@COMUNE.MESERO.MI.IT

Contitolare del trattamento
Il Comune di Marcallo con Casone rappresentato pro tempore dal Sindaco.
Indirizzo:Via Vitali 18, Marcallo con Casone 20010 (MI)
Email: **SEGRETERIA@MARCALLO.it;**

CONTITOLARE

Finalità del trattamento

1. 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" e delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del D.lgs. 267/2000;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;
2. vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
3. tutelare l'ordine, il decoro e la quiete pubblica;
4. controllare aree specifiche del territorio comunale;
5. monitorare i flussi di traffico;
6. verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici;
7. attivare uno strumento operativo di protezione civile sul territorio comunale.

BASI GIURIDICHE

Basi giuridiche per le attività svolte dal comune possono essere:
Necessità di

a. salvaguardare degli interessi vitali dell'interessato o di

RPD/DPO

Responsabile per la protezione dei dati (RPD/DPO)

Gli interessati possono contattare il Responsabile della Protezione dei Dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti sopra indicati.

	un'altra persona fisica b. svolgere compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune.		Il Responsabile per la Protezione dei Dati è contattabile all'indirizzo: dpo-privacy@comune.mesero.mi.it rpd@marcallo.it
 **CATEGORIE DI DATI**	**Tipologie dei dati trattati** Le tipologie di dati sono quelle coinvolte nelle Videoregistrazioni (immagine personale, targhe, ecc.)	 **DATI SENSIBILI**	**Dati "sensibili"** **Categorie particolari di dati e relativi a reati** Queste tipologie di dati possono essere trattate in quanto necessari per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione essendo proporzionato alla finalità perseguita, rispettando l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato
 **CONSERVAZIONE**	Il Titolare **applica il principio di minimizzazione dei dati** per tutti i trattamenti. La **conservazione standard** è di 7 giorni**,** salvo necessità di aumento dovuto al legittimo perseguimento degli scopi dichiarati, e come tale disciplinato nel Regolamento interno. Le registrazioni delle videocamere che rientrano nella disciplina dello Statuto dei Lavoratori adeguano il periodo di Data Retention alle disposizioni normative (24-72 ore). Eventuali **aree sottoposte** a videosorveglianza sono **indicate da appositi cartelli**.	 **DESTINATARI EVENTUALI**	**Soggetti che possono trattare i dati** ✓ **Autorizzati** al trattamento debitamente **istruiti** e tenuti alla riservatezza (ad es. i dipendenti del Comune) ✓ **Responsabili** del trattamento che hanno sottoscritto **accordi vincolanti** secondo la normativa Europea (fornitori di servizi informatici come il sito internet, sistemi di prenotazione online, di pratiche anagrafiche, pratiche edilizie, ecc.). ✓ **Titolari autonomi** con una valida base giuridica per farlo (ad es. Autorità Giudiziarie e di Pubblica Sicurezza, Regione, Consulenti Legali e Autorità amministrative).

PAESI TERZI EXTRA UE-SEE

Trasferimento dati in Paesi terzi

Il Comune non trasferisce i dati in Paesi extra UE.

Qualora fosse necessario e il Comune abbia adeguata base giuridica **e*ventuali trasferimenti in Paesi* extra UE *avverranno in conformità alla normativa vigente:***

- ✓ in paesi riconosciuti come sicuri dalla Commissione UE
- ✓ in paesi con i quali l'Europa abbia accordi Internazionali sulla protezione dei dati
- ✓ con soggetti con cui il Titolare abbia stipulato accordi giuridicamente vincolanti atti a fornire garanzie adeguate per la protezione degli Interessati come previsto dalla normativa
- ✓ in presenza di deroghe previste quale, ad es. il consenso dell'interessato
- ✓ per necessità e non in modo ripetitivo per tipologie e quantità di dati che lo permettono.

DIRITTI

Diritti degli Interessati

- ✓ Ottenere la **conferma** o meno di un trattamento in corso ed eventualmente ottenere accesso ai dati che riguardano l'interessato
- ✓ Conoscere l'**origine** dei dati trattati dal Titolare
- ✓ **Verificare l'esattezza** dei dati che riguardano l'interessato
- ✓ Opporsi, per motivi legittimi, al trattamento
- ✓ **Chiedere eventuale**
  - l'integrazione
  - cancellazione
  - aggiornamento
  - rettifica
  - blocco dei dati personali trattati in violazione di legge
  - portabilità

Le richieste possono essere rivolte al Titolare o al Responsabile per la Protezione dei Dati.

Gli interessati hanno altresì il diritto di

- ✓ Essere informati su violazioni che possono presentare un alto rischio per gli interessati stessi
- ✓ Proporre reclamo all'Autorità di controllo competente nello Stato membro in cui risiedono abitualmente o lavorano o dello Stato in cui si è verificata la presunta violazione

Allegato 4: Misure di sicurezza per i dati

1. Il/i monitor/s degli impianti di videosorveglianza devono essere collocati in moda tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

2. L'accesso alle immagini da parte dei soggetti autorizzati e legittimati al trattamento deve limitarsi alle attività oggetto della sorveglianza; eventuali altre informazioni di cui vengono a conoscenza, mentre osservano il comportamento di un soggetto ripreso, devono essere ignorate.

3. Nel caso le immagini siano conservate, i relativi supporti tecnologici devono essere custoditi, per la durata della conservazione, in un armadio (o simile struttura) dotato di serratura, apribile solo dal soggetto autorizzato.

4. La cancellazione delle immagini avverrà automaticamente scaduti i 7 giorni per le telecamere che lo prevedono. Per le tipologie individuate nell'inventory con diverso periodo di conservazione questo sarà in alcuni casi automatico oppure manuale.

5. Nel caso il supporto debba essere sostituito per eccessiva usura, dovrà essere distrutto in modo che non possa essere più utilizzabile, né che possano essere recuperati dati in esso presenti nel rispetto del provvedimento del Garante specifico e secondo le migliori pratiche suggerite dallo stato dell'arte e della tecnica.

6. L'accesso alle immagini è consentito solo:

- ai soggetti autorizzati e legittimati allo specifico trattamento;
- per indagini delle autorità giudiziarie o di polizia;
- all'Amministratore di Sistema del Comune di MARCALLO CON CASONE o di MESERO e alla ditta fornitrice dell'impianto nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione;
- al terzo, legittimato, in quanto oggetto delle riprese o suo verificato delegato.

7. Nel caso di accesso alle immagini per indagini delle Autorità Giudiziarie o di Polizia, opportuno informare il Titolare e il DPO.

8. Nel caso di accesso alle immagini del terzo, debitamente autorizzato, questi dovrà avere visione solo delle immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà essere utilizzata, da parte dell'incaricato al trattamento, una schermatura del video, tramite apposito strumento.

9. Tutti gli accessi dovranno essere registrati mediante l'annotazione di apposito registro, predisposto secondo lo schema qui allegato, nel quale dovranno comunque essere

riportati:
- la data e l’ora dell’accesso;
- l’identificazione del terzo autorizzato
- gli estremi dell’autorizzazione all’accesso.

Allegato 5: Procedura per l'accesso alle immagini ed esercizio dei diritti.

1. raccogliere l'istanza attraverso la compilazione del formulario (**Allegato 5.1**) e bloccare la cancellazione per i dati richiesti
2. dare riscontro all'istanza (es. via e-mail con una conferma di ricezione richiesta o con il cartaceo con una copia della richiesta con timbro della PL sulla data)
3. valutare l'istanza:
    a. legittimità del richiedente
    b. legittimità della richiesta
    c. pertinenza della richiesta
    d. ripetitività
    e. chiedere intervento DPO se opportuno
4. dare seguito all'istanza:
    a. valutando se necessario chiedere informazioni integrative
    b. estrarre i dati
    c. trasmetterei dati
5. attendere 36 ore prima di chiudere l'istanza e cancellare i dati

Allegato 5.1: Formulario per esercizio di diritti
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI ESERCITABILI PER IL TRATTAMENTO DI VIDEOSORVEGLIANZA IN CONSIDERAZIONE DELLE BASI GIURIDICHE UTILIZZATE
(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a…….
nato/a a……..il……., esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali
(art. 15 del Regolamento (UE) 2016/679)
Il sottoscritto *(barrare solo le caselle che interessano)*:

- ☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
- ☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;
    - o le finalità del trattamento;
    - o le categorie di dati personali trattate;
    - o i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
    - o il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
    - o l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
    - o l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati
(artt. 16-18 del Regolamento (UE) 2016/679)
Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

- ☐ **interrompere il procedimento di cancellazione automatico fino alla valutazione ultima della richiesta nel periodo intercorrente fino ad un massimo di 7 giorni precedenti alla presente richiesta.**
- ☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);
- ☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:
    - a)
    - b)
- ☐ nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;

- ☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:
  - ☐ il trattamento dei dati è illecito;
  - ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____

3.Portabilità dei dati[1]
(art. 20 del Regolamento (UE) 2016/679)
Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

- ☐ **ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;**
- ☐ trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: ……..):*
- ☐ tutti i dati personali forniti al titolare;
- ☐ un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento <u>es. videocamera posizionata in …. Nel periodo di….):</u>

_____
_____
_____
_____
_____
_____
_____

Il sottoscritto:

- ☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

[1] Per approfondimenti: Linee-guida sul diritto alla "portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.

- ☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

_____

Recapito per la risposta[2]:
Via/Piazza
Comune **Provincia** **Codice postale**
oppure
e-mail/PEC:

Eventuali precisazioni
Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):
_____
_____
_____
_____
_____
_____
_____

(Luogo e data) (Firma)

[2] Allegare copia di un documento di riconoscimento

Allegato 6: Soggetti autorizzati al trattamento dei dati personali

ESTERNI	
Titolari autonomi	• Forze di Polizia Legittimate • Autorità Giudiziarie
Responsabili del Trattamento	• Computer Design • Enet Solution • Halley Informatica
Amministratori di sistema	• Computer Design • Enet Solution • Halley Informatica
INTERNI	
Amministratori di sistema	N/A
Incaricati	• Antonio Schintu • Filippo Corallo • Pasquale Polito • Gianluca Travaglino • Elena Panceri • Luca Colombo • Colli Marco

Allegato 7: Registro degli accessi alla visione delle immagini videoregistrate.

Nome e Cognome o Autorità	Documento identità	Estremi Autorizzazione o richiesta	Ora di entrata	Ora di uscita	Dichiarazione	Firma e data
					Dichiaro di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale, ai sensi della vigente normativa sulla privacy.	
					Dichiaro di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale, ai sensi della vigente normativa sulla privacy.	
					Dichiaro di mantenere l'assoluta riservatezza su qualunque dato personale di cui possa essere venuto a conoscenza durante la permanenza nel locale, ai sensi della vigente normativa sulla privacy.	

Allegato 8: Pagina di Registro delle attività di trattamento

Registro delle attività di Trattamento
del Titolare COMUNE DI MARCALLO CON CASONE
Via Vitali 18, 20010 Marcallo con Casone (MI) Italia
e MESERO Via San Bernardo 41, 20010 Mesero (MI) - Italia

SCHEDA 1 DESCRIZIONE DEL TRATTAMENTO	GESTIONE DEI DATI PERSONALI IN RELAZIONE AL SISTEMA DI VIDEOSORVEGLIANZA
FINALITÀ DEL TRATTAMENTO	L'utilizzo degli impianti di videosorveglianza è finalizzato a: 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" e delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del D.lgs. 267/2000; b) 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; c) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato; d) tutelare l'ordine, il decoro e la quiete pubblica; e) controllare aree specifiche del territorio comunale; f) monitorare i flussi di traffico; g) verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici; h) attivare uno strumento operativo di protezione civile sul territorio comunale.
DESCRIZIONE CATEGORIE INTERESSATI	Interessati che transitano nelle zone sottoposte a videosorveglianza.
DESCRIZIONE CATEGORIE DATI PERSONALI	Immagini • degli interessati (dati comuni es. tratti somatici, dati particolari es. dati che rilevano lo stato di salute, dati relativi a reati es. flagranza). • di codici identificativi (targhe)
CATEGORIE DI DESTINATARI A CUI I DATI VENGONO COMUNICATI	Tutti i soggetti legittimati da una base giuridica valida a titolo esemplificativo e non esaustivo: fornitori IT, Consulenti, Legali per difesa in giudizio, Amministratori di sistema, Titolari autonomi quali enti e Pubbliche Amministrazioni destinatari di comunicazioni obbligatorie.
PAESI TERZI COINVOLTI NEL TRATTAMENTO E RELATIVE BASI GIURIDICHE APPLICATE	I dati Personali saranno trattati dal Titolare all'interno dell'Unione Europea e conservati su server ubicati all'interno dell'Unione Europea. Eventuali trasferimenti operati dai destinatari dei dati saranno da considerarsi come trattamenti di autonoma titolarità svolti dai soggetti.
DATA RETENTION	I dati saranno conservati per un periodo congruo, nel rispetto dei principi di proporzionalità e necessità, fino a che non siano state perseguite le finalità del trattamento indicate. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione (secondo l'art. 6, co. 8, del D.L. 23/02/2009, n. 11 nell'ambito dell'utilizzo da parte dei Comuni di sistemi di

	videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana). Le registrazioni delle videocamere che rientrano nella disciplina dello Statuto dei Lavoratori adeguano il periodo di Data Retention alle disposizioni normative (24-72 ore).
MISURE DI PROTEZIONE	Cifratura: applicata alle informazioni conservate a riposo e alle pagine di accesso ai siti internet. Capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento tramite misure generali: Firewall, antivirus, misure di sicurezza fisiche, access log, password complesse per le utenze. Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico tramite ripristino dei Backup del sistema strutturati secondo le tempistiche e le procedure indicate in “tabella Backup”. Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza dei dati. **Le misure di protezione saranno adeguate alle disposizioni delle linee guida AGiD vigenti.**