



Città di **GALLARATE**

Regolamento dei sistemi di videosorveglianza del Comune di Gallarate

Anno 2022

Approvato con delibera C.C. n. 25 del 23/05/2022

CAPO I - DISPOSIZIONI GENERALI

- ART. 1 - OGGETTO
- ART. 2 - NORME DI RIFERIMENTO E PRINCIPI GENERALI
- ART. 3 - FINALITA'
- ART. 4 - DEFINIZIONI
- ART. 5 - INFORMATIVA

CAPO II- SOGGETTI E COMPITI DEI SOGGETTI

- ART. 6 -TITOLARE
- ART. 7 – SUPERVISORE E RESPONSABILI DEL TRATTAMENTO DEI DATI
- ART. 8 - SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI
- ART. 9 - SOGGETTI ESTERNI

CAPO III - TRATTAMENTO DEI DATI PERSONALI

- ART. 10 - MODALITÀ DI RACCOLTA, TRATTAMENTO E CONSERVAZIONE DEI DATI
- ART. 11 - UTILIZZO DI PARTICOLARI SISTEMI MOBILI
- ART. 12 - DIRITTI DELL'INTERESSATO

CAPO IV - MISURE DI SICUREZZA E ACCESSO

- ART. 13 - SICUREZZA DEI DATI
- ART. 14 - ACCESSO ALLE CENTRALI DI CONTROLLO
- ART. 15 - ACCESSO AGLI IMPIANTI E AI DATI

CAPO V- SISTEMI INTEGRATI DI VIDEOSORVEGLIANZA

- ART. 16 - SISTEMA INTEGRATO DI VIDEOSORVEGLIANZA TRA PUBBLICO E PRIVATO
- ART. 17 - PARTNERIATO PUBBLICO PRIVATO PER IL POTENZIAMENTO DELLA VIDEOSORVEGLIANZA AD USO PUBBLICO

CAPO VI - TUTELA AMMINISTRATIVA E GIURISDIZIONALE

- ART. 18 - MEZZI DI RICORSO, TUTELA AMMINISTRATIVA E TUTELA GIURISDIZIONALE
- ART. 19 - DIRITTO AL RISARCIMENTO, RESPONSABILITA' E DANNI CAGIONATI PER EFFETTO DEL TRATTAMENTO DI DATI PERSONALI

CAPO VII - DISPOSIZIONI FINALI

- ART. 20- ENTRATA IN VIGORE

CAPO I - DISPOSIZIONI GENERALI

Art. 1 - Oggetto

1. Il presente Regolamento disciplina il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza attivati nel territorio del Comune di Gallarate (VA). Disciplina il trattamento degli ulteriori dati acquisiti per mezzo degli apparecchi di ripresa portatili (*dashcam*, *bodycam*, altri apparati mobili e radio), anche concernenti la localizzazione geografica. Garantisce che il trattamento dei dati personali, effettuato mediante i predetti sistemi, gestiti ed impiegati dal Comune di Gallarate e dai soggetti delegati nel territorio comunale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, anche lavoratori, con particolare riferimento alla riservatezza e all'identità personale.

2. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in diretta ed in remoto, realizzata mediante sistemi di ripresa video, captazione di immagini, ed eventuale analisi, collegati ad un centro di controllo, compresa la localizzazione geografica.

3. In particolare, il presente Regolamento:

- a) definisce le modalità di utilizzo degli impianti di videosorveglianza;
- b) 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;
- c) definisce gli ulteriori strumenti di acquisizione di immagini e dati in possibile dotazione all'Ente;
- d) delinea i principi per le procedure da adottarsi, per mezzo di disciplinari e linee guida, per il trattamento dei dati e che assicurino, fin dalla fase della progettazione, la pertinenza e non eccedenza dei dati raccolti rispetto alle finalità, garantendo la massima informatizzazione e digitalizzazione di ogni azione e processo ed affinché venga assicurato il rispetto del sistema di gestione per la qualità.

4. Gli impianti di videosorveglianza attivati nel Comune di Gallarate riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese.

5. Sono attivabili impianti di foto-sorveglianza e videosorveglianza mobili, posizionabili in aree del territorio comunale e per specifici servizi individuati dal Corpo di Polizia Locale di Gallarate (*cd* foto-video trappole) oppure montati su veicoli di servizio e utilizzabili per le finalità indicate nell'art. 3, comma 3, lettere *a)*, *b)*, *c)*, *d)*, *e)*, *h)* e *i)* del presente Regolamento.

Sono attivabili sistemi di foto-video ripresa da trasporto personale (*bodycam*) o veicolare (*dashcam*) finalizzati alla sicurezza personale, alla tutela dell'incolumità pubblica e degli operatori di Polizia Locale. Sono altresì collegabili al sistema di videosorveglianza comunale i sistemi privati, gestiti in via esclusiva dai soggetti dell'Ente, senza possibilità per i privati stessi di accedere ai dati, nel rispetto degli artt. 16 e 17 del presente Regolamento, previo disciplinare redatto dal titolare del trattamento o, per suo conto, dal Dirigente Comandante la Polizia Locale, e sottoscritto dal soggetto privato.

6. L'utilizzo di sistemi di ripresa foto-videografica, anche installati su aeromobili a pilotaggio remoto (droni), per le finalità di polizia, è disciplinato dal Capo V del DPR n. 15 del 15/01/2018 recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e

comandi di polizia” e ss.mm.ii, dal D.lgs 101/2018 e dal D.lgs 51/2018, anche in coordinamento con la normativa ENAC e con il Codice della Navigazione.

7. Il sistema di videosorveglianza del Comune di Gallarate è integrato con le apparecchiature di rilevazione delle targhe dei veicoli in transito (portali / varchi di lettura targhe), apposte principalmente lungo i varchi di accesso perimetrali alla rete viaria cittadina. La disciplina relativa al trattamento dati di cui al presente Regolamento si applica anche a tali apparecchi, in quanto e nei limiti in cui consentono la ripresa delle immagini e la registrazione dei dati alfanumerici contenuti nelle targhe veicolari.

8. L'utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della Strada (es. *autovelox*, *telelaser*, ecc...), in considerazione della peculiarità dei fini istituzionali perseguiti, non è assoggettato alla completa disciplina di cui al presente Regolamento, ma alle disposizioni dettate dal Garante della *privacy* nel decalogo dell'8 aprile 2010 al paragrafo 5.3 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 GDPR o 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”*;
- Decreto Legislativo 30 giugno 2003, n. 196 recante il *“Codice in materia di protezione dei dati personali”* e ss.mm. e ii., tra cui il Decreto Legislativo 10 agosto 2018, n. 101, recante *“Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016”*;
- 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”* e Decreto Legislativo 18 maggio 2018, n. 51;
- DPR n. 15 del 15/01/2018 recante *“Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia”*;
- 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);
- Linee guida EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020, ed eventuali successive ulteriori modifiche o integrazioni;
- Decreto Legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48, recante *“Disposizioni urgenti in materia di sicurezza delle città”*;
- Decreto legislativo 7 marzo 2005, n. 82 e ss.mm.ii recante il *“Codice dell'Amministrazione Digitale”*;
- Regolamento (UE) 910/2014 recante *“electronic IDentification Authentication and Signature”*, sulla firma, autenticazione ed identificazione elettronica (Regolamento eIDAS).

2. La videosorveglianza in ambito comunale si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5, GDPR e, in particolare:

- Principio di liceità. Il trattamento di dati personali da parte di soggetti pubblici è lecito allorché 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 (*cd* 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, devono essere 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, 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, fin dalla fase di progettazione del sistema e deve essere sempre garantita la revisione della valutazione, al fine di verificare il persistere delle condizioni di necessità. 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. Non possono essere utilizzati i sistemi di videosorveglianza comunale al fine di controllare o per monitorare l'attività dei lavoratori. Questi potranno essere dotati di sistemi di foto-video ripresa o localizzazione portatili, anche connessi a sistemi radiotrasmittenti, per ragioni connesse alla tutela della loro sicurezza ed incolumità.
- 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 - Finalità

1. Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono quelle concernenti le funzioni istituzionali demandate al Corpo di Polizia Locale di Gallarate dalla legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Municipale, dalla Legge regionale n. 6/2015, dallo Statuto e dal vigente Regolamento comunale, nonché dal decreto legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 "*Disposizioni urgenti in materia di sicurezza delle città*" e dalle altre disposizioni normative applicabili al Comune di Gallarate. In particolare, l'uso di impianti di

videosorveglianza è strumento per l'attuazione di un sistema integrato di politiche per la sicurezza urbana, come definita dalle fonti normative sopra citate e successive *mm* e *ii*.

2. Ogni azione, comunicazione o processo posto in essere dovrà essere attuato garantendo la massima informatizzazione e digitalizzazione e non è consentito l'utilizzo di registri, sistemi, annotazioni o archivi di ogni genere realizzati o mantenuti in modalità cartacea.

3. L'utilizzo degli impianti di videosorveglianza è finalizzato a:

a) prevenire e reprimere attività illecite, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 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.lvo 267/2000, fatte salve le competenze in materia di ordine pubblico di spettanza dell'autorità di P.S.;

b) prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado urbano, controllo delle aree dismesse 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 e dirigenziali, anche in riferimento alla L. 689/1981 e con le facoltà ammesse dall'art. 13 della predetta L. 689;

c) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato, compresi gli edifici, le pertinenze e i beni in disponibilità all'Ente, in particolare la sede del Corpo di Polizia Locale e del sistema di protezione civile;

d) tutelare il decoro e la quiete pubblica;

e) controllare aree specifiche del territorio comunale, anche in relazione a zone sensibili per la possibile incidentalità ed infortunistica;

f) monitorare i flussi di traffico e monitorare l'accesso alle zone a traffico limitato (ZTL) o eventuali aree pedonali o di rilevanza urbana. A tal fine, è consentita la visualizzazione delle specifiche camere dedicate anche agli appartenenti, nominativamente incaricati, dell'ufficio tecnico del traffico;

g) verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici;

h) attivare uno strumento operativo di protezione civile sul territorio comunale, garantendo l'impiego di camere, fisse o mobili, anche SAPR, per le attività di cui al D.lgvo 2 gennaio 2018, n. 1. A titolo esemplificativo, attivare sistemi di monitoraggio dei sottopassaggi e di controllo di eventuali allagamenti;

i) tutelare l'incolumità e la sicurezza degli operatori di polizia locale.

4. Il sistema di videosorveglianza in uso presso il Comando di Polizia Locale di Gallarate è di tipo "integrato", consentendo l'utilizzo condiviso con il Commissariato di Pubblica Sicurezza, con il Comando Compagnia Carabinieri di Gallarate ed eventualmente con altre Forze dell'Ordine, quale strumento di prevenzione e di razionalizzazione dell'azione di polizia su tutto il territorio. Nel caso, i soggetti predetti dovranno essere nominati quali Responsabili del trattamento e dovranno rispettare quanto contenuto nel presente Regolamento.

Il sistema di videosorveglianza è integrato e connesso alla centrale operativa unificata di protezione civile e del Comando di Polizia Locale di Gallarate.

5. 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.

6. Per le finalità sopra indicate, possono essere trasmesse all'impianto di videosorveglianza e alle apparecchiature in uso alla centrale operativa anche le immagini raccolte dai sistemi APR (droni), compresa la visualizzazione *live* (in diretta - *streaming*).

7. Ogni attività dovrà compiersi nel rispetto dei principi di:

- *digital & mobile first* (digitale e mobile come prima opzione): l'Ente deve realizzare servizi primariamente digitali;
- *cloud first* (*cloud* come prima opzione): in fase di definizione di un nuovo progetto o di sviluppo e integrazione del progetto e servizio esistente, dovrà essere adottato primariamente il paradigma *cloud*, tenendo conto della necessità di prevenire il rischio di *lock-in*.

8. Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300, 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. I lavoratori possono essere dotati di strumenti che consentano la localizzazione geografica, anche attraverso sistemi radio, che possa consentirne anche la rappresentazione su mappe digitali, nonché abilitati alle riprese video a tutela della loro sicurezza e per una migliore gestione degli interventi sul territorio.

9. Gli impianti di videosorveglianza non possono essere utilizzati per l'irrogazione di sanzioni per infrazioni al Codice della Strada, essendo all'uopo prevista disciplina specifica. Possono essere utilizzati per l'eventuale invio sul posto da parte delle Centrali Operative di personale con qualifica di organo di polizia stradale, per le contestazioni delle violazioni ai sensi del Codice della Strada.

Art. 4 - Definizioni

1. Ai fini del presente Regolamento, si richiamano le definizioni contenute nel GDPR Reg. (UE) 2016/679 (Art. 4). In aggiunta, si intende:

- a) per «*interessato*», la persona fisica identificata o identificabile cui si riferiscono i dati personali oggetto di trattamento [punto 1) del Reg. (UE)];
- b) per «*incaricato del trattamento*», la persona fisica che sia stata autorizzata dal titolare del trattamento, dal supervisore o dal responsabile del trattamento e che abbia accesso a dati personali e che esegua il trattamento;
- c) per «*supervisore*», il Dirigente la Polizia Locale, settore al quale afferiscono gli impianti di videosorveglianza;
- d) per «*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;
- e) per «*diffusione*», il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- f) per «*dato anonimo*», il dato che in origine, o a seguito di processo di trattamento, non può essere associato ad un interessato identificato o identificabile;
- g) per «*impianti di videosorveglianza*», salve ove diversamente indicato, gli impianti e sistemi di videosorveglianza, fissi o mobili, anche in uso personale o veicolare. Gli impianti di videosorveglianza

lavorano in stretta interconnessione con le apparecchiature in uso agli operatori e al servizio della Centrale Operativa unificata di protezione civile e Polizia Locale del Comune di Gallarate, compresi i sistemi di geolocalizzazione. Consentono di riprendere e registrare immagini e suoni, nonché possono consentire la localizzazione geografica, anche mediate sistemi radioconnessi;

h) per «*disciplinare*», le disposizioni tecniche e tecnico-organizzative impartite dal titolare del trattamento dei dati, dal supervisore o dal responsabile del trattamento dei dati;

i) per «*linea guida*», le indicazioni tecniche e tecnico-organizzative emanate dal responsabile per la protezione dei dati anche al fine di informare e formare gli incaricati – soggetti autorizzati al trattamento, e fornire consulenza al titolare del trattamento, al supervisore o al responsabile del trattamento, nonché agli incaricati e dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento;

l) per «*audit*», la valutazione interna svolta dal responsabile della protezione dei dati o la valutazione esterna svolta da un organismo terzo volta a rilevare il rispetto delle procedure predisposte, i ruoli e i doveri per assicurare la qualità delle azioni e il rispetto dei diritti delle persone fisiche con riferimento ai dati personali e se gli obiettivi siano correttamente gestiti e perseguiti. Nella valutazione verranno considerate le disposizioni e le indicazioni fornite attraverso i disciplinari e le linee guida, seguendo le norme della UNI EN ISO 19011 e successivi aggiornamenti della stessa.

2. Ulteriori definizioni sono contenute nel CAD D.lvo 82/2005 e *ss.mm. e ii.*, nel Regolamento (UE) 910/2014 (eIDAS - *Electronic Identification and Trust Services Regulation*) e, in aggiunta, si intende:

m) per «*informatizzazione*», l'introduzione dei sistemi informatici in uno o più settori di attività, con la conseguente eliminazione delle operazioni manuali;

n) per «*dematerializzazione*», la trasformazione del documento cartaceo in digitale, operazione che consente costi minori ed una più agevole trasmissione e modifica del documento;

o) per «*digitalizzazione*» è il processo organizzativo che rende disponibili i documenti all'interno dell'ente su supporti digitali e non più cartacei, con perdita di fisicità del documento.

Art. 5 - Informativa

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

2. A tal fine l'Ente utilizzerà lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, riportato in *fac-simile* nell'allegato n. 1 del Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010, come modificate e integrate dalle Linee guida EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020, ed eventuali successive ulteriori modifiche o integrazioni.

3. L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le 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 ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante il sito *internet* istituzionale dell'Ente e altri mezzi di diffusione locale. Cura la trasmissione alle Autorità dell'elenco dei siti di ripresa, se prevista.

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.

CAPO II- SOGGETTI E COMPITI DEI SOGGETTI

Art. 6 - Titolare

1. Il Comune di Gallarate è titolare del trattamento dei dati personali acquisiti mediante utilizzo degli impianti di videosorveglianza di cui al presente Regolamento, compresi i dati di geolocalizzazione.

2. Al titolare competono i compiti e svolge le attività previste dal RGPD. Compete la preliminare decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza, nell'ambito delle finalità previste nel presente Regolamento. Promuove un sistema di gestione per la qualità rispettoso dello *standard* ISO 9001 e l'adesione a codici di condotta.

Art. 7 – Supervisore e Responsabili dei dati trattati

1. Il Dirigente Comandante del Corpo di Polizia Locale di Gallarate è Supervisore del trattamento di dati personali effettuato mediante l'utilizzo degli impianti di cui al presente Regolamento. La nomina è effettuata con atto dell'Ente, quale titolare del trattamento, nel quale sono analiticamente specificati i compiti affidati.

2. Il Dirigente Comandante la Polizia Locale è coadiuvato dai responsabili del procedimento nominati con atto di micro organizzazione del Settore, a cui è affidata l'attuazione dei compiti in cura, soggetti autorizzati al trattamento.

3. Il Supervisore nomina eventuali soggetti esterni, in qualità di responsabili del trattamento, per lo svolgimento di attività correlate alla gestione ed al funzionamento dei sistemi che potrebbero comportare, seppur occasionalmente o incidentalmente, un trattamento di dati. Il riferimento, contenuto nel presente Regolamento, ai "Responsabili del trattamento" è da intendersi a Responsabili esterni all'organizzazione.

4. In particolare, il Supervisore del trattamento:

- individua e nomina, con propri atti, gli incaricati quali soggetti autorizzati al trattamento, definendo differenti e graduate possibilità di accesso, impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di

cui all'art. 29, RGPD; detti soggetti sono opportunamente istruiti e formati con riferimento alla tutela del diritto alla riservatezza, 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, nonché alle procedure per assicurare il rispetto del sistema di gestione per la qualità;

- con disciplinare, individuerà i differenti livelli di trattamento a cui potranno accedere gli incaricati, quali soggetti autorizzati;
- individua e nomina, con proprio atto, il responsabile della protezione dei dati (RPD), qualora non sia stato nominato dal titolare del trattamento;
- assicura che sia resa disponibile l'informativa "minima" agli interessati, secondo quanto definito al precedente art. 5;
- 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;
- assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- 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;
- 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;
- 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;
- 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;
- 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;
- unitamente al responsabile della protezione, 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;
- unitamente al responsabile della protezione, assiste il titolare nell'effettuazione della valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e del precedente art. 6 del presente Regolamento e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;
- attua un sistema di gestione per la qualità nel rispetto della norma ISO 9001, predisponendo periodici *audit* sia interni che esterni, con la collaborazione del responsabile per la protezione dei dati;
- 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 formato elettronico, anche attraverso *software* e *tools* dedicati;

- garantisce che il responsabile della protezione dei dati designato 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 e la formazione specifica;
- 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;
- 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;
- assicura, anche adottando opportuni disciplinari tecnico-organizzativi, che le attività, azioni e processi siano effettuati garantendo la massima digitalizzazione, informatizzazione e dematerializzazione, utilizzando gli strumenti offerti dalla tecnologia informatica e della comunicazione;
- assicura che i soggetti autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito, garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali e vigila affinché le mansioni svolte vengano effettuate utilizzando i sistemi informatici e telematici;
- garantisce la tempestiva emanazione, per iscritto, di disciplinari ed ordini di servizio rivolti al personale e soggetti autorizzati con riferimento ai trattamenti realizzati mediante gli impianti 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;
- vigila sul rispetto da parte dei soggetti autorizzati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

5. I Responsabili del trattamento, in particolare, sono nominati con atto giuridico in cui siano specificati obblighi e responsabilità, ai sensi degli artt. 28 e 29 RGPD. La regolamentazione di tali impegni può essere formalizzata dal Supervisore a cui compete anche aggiornare periodicamente la lista dei responsabili del trattamento.

6. I soggetti nominati responsabili del trattamento devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato.

Art. 8 - Soggetti autorizzati al trattamento dei dati personali

1. Il Dirigente Comandante del Corpo di Polizia Locale, quale Supervisore del trattamento per conto del titolare, nomina i soggetti autorizzati al trattamento dei dati, in numero sufficiente a garantire la regolarità del servizio turnato.

L'autorizzazione è effettuata con atto scritto, nel quale sono analiticamente specificati i compiti affidati agli incaricati, quali soggetti autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, anche facendo riferimento ad apposito disciplinare preventivamente emanato.

2. I soggetti autorizzati hanno diverse possibilità di accesso, dalla mera visione delle immagini, alla possibilità di effettuare modifiche alle riprese o alle impostazioni dei sistemi, secondo un sistema graduato di accesso e trattamento a cui i diversi soggetti autorizzati possono essere abilitati.

3. Il salvataggio e la comunicazione dei dati potrà essere effettuato solo da un limitato e ristretto numero di soggetti incaricati, sotto la direzione dei responsabili del procedimento secondo le normative interne

all'Ente. È loro cura la corretta compilazione di un registro delle operazioni, sotto la diretta responsabilità del supervisore.

4. Il disciplinare emanato dal supervisore assicura che ogni operatore addetto ordinariamente alle funzioni integrate di centrale operativa unificata e videosorveglianza sia designato tra gli appartenenti al Corpo di Polizia Locale che, per esperienza, capacità e affidabilità, fornisca idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati, nonché garanzia di rispetto del sistema di gestione per la qualità.

5. I soggetti autorizzati devono:

- a) per l'accesso alle immagini e alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, astenendosi dall'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, dalla postazione di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento. Non è consentito l'utilizzo di *password* condivise;
- b) 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;
- c) mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle proprie mansioni e funzioni istituzionali;
- d) 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;
- e) astenersi dal creare banche dati nuove, senza espressa e motivata autorizzazione del titolare del trattamento o, per lui, del supervisore;
- f) conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
- g) evitare l'utilizzo di *account* di accesso condivisi e limitare l'accesso a cartelle e *files* condivisi ai soli soggetti che, nel rispetto delle finalità, debbano trattare i dati in essi contenuti;
- h) fornire al titolare, al supervisore 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;
- i) rispettare scrupolosamente le istruzioni del titolare del trattamento, i disciplinari del supervisore o dei responsabili del trattamento e le linee guida emesse dal responsabile per la protezione dei dati;
- l) utilizzare dispositivi di supporto fisico esclusivamente messi a disposizione dall'Ente e preferire, comunque, servizi di *clouding* e di trasferimento *web*, assicurandosi che i fornitori di tali servizi rispettino adeguati livelli di *privacy policy*;
- m) non utilizzare supporti cartacei che contengano dati personali, salvo casi di motivata necessità e ammessi dal supervisore;
- n) rispettare scrupolosamente le istruzioni impartite per il corretto trattamento dei dati e per minimizzare i rischi di compromissione della sicurezza informatica.

6. Tra i soggetti autorizzati al trattamento vengono individuati gli operatori cui è affidata la custodia e la conservazione delle chiavi di accesso agli armadi per la conservazione dei supporti magnetici, in numero sufficiente ad assicurare la pronta disponibilità all'accesso.

Sono altresì nominati tra essi i responsabili della gestione tecnica degli impianti di videosorveglianza autorizzati al trattamento per i compiti relativi al ruolo, ad interfaccia con le Società eventualmente incaricate della manutenzione degli impianti, abilitate a trattare i dati previo incarico come responsabili del trattamento.

7. 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 e agli specifici disciplinari emanati dal supervisore. In particolare, sono stabilite con disciplinare le modalità e limiti per l'utilizzo dei dispositivi mobili (*bodycam, dashcam, tablet-smartphone*, foto-video trappole, ecc...) e dei SAPR, con modalità che garantiscano sempre il più ampio impiego degli strumenti informatici e telematici e divieto di utilizzo ordinario di strumenti cartacei.

Art. 9 - Soggetti esterni

1. Il supervisore, svolgendo per conto del titolare mansioni di coordinamento nell'ambito del trattamento dei dati, è autorizzato a ricorrere ad addetti esterni, quali responsabili del trattamento, che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate tali da assicurare la tutela dei diritti dell'interessato.

2. È possibile il ricorso a soggetti esterni in tutti i casi in cui egli, per la gestione/assistenza del sistema di videosorveglianza, debba affidare incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente.

3. Qualora tra le mansioni del responsabile del trattamento (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.

CAPO III - TRATTAMENTO DEI DATI PERSONALI

Art. 10 - Modalità di raccolta, trattamento e conservazione dei dati

1. L'installazione delle telecamere avviene nei luoghi pubblici (strade, piazze, immobili) in conformità all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale, sentito il Dirigente Comandante la Polizia Locale di Gallarate.

2. L'utilizzo del brandeggio, dello *zoom* o di altri accorgimenti tecnici di puntamento degli obiettivi da parte dei soggetti autorizzati avviene nel rispetto dei principi e delle finalità contenuti nel presente Regolamento e delle abilitazioni ammesse per i singoli soggetti abilitati.

3. 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.

4. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato o ad esigenze di indagine della polizia giudiziaria o disposte dall'Autorità Giudiziaria. I segnali video delle unità di ripresa sono inviati presso la sede del Corpo di Polizia Locale di Gallarate in centrale operativa unificata o altro *data center* individuato appositamente dove sono registrati su appositi *server*. Il segnale

è reso disponibile ad altre centrali operative, del Commissariato di Pubblica Sicurezza, del Comando Compagnia Carabinieri o altre Forze dell'Ordine a ciò autorizzate, previa nomina come responsabili del trattamento. Nelle sedi predette le immagini sono visualizzate su *monitor* e *hardware client* appositamente configurati. L'accesso ai locali *server* e *data center* è strettamente riservato ai soggetti nominati. L'accesso è sempre consentito ai responsabili della gestione tecnica degli impianti, al titolare e supervisore del trattamento, nonché al responsabile della protezione dei dati.

5. I dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per le finalità di cui all'art. 3 del 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, esatto e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- sottoposti a procedura di anonimizzazione o pseudonomizzazione qualora non sia necessario avere a disposizione dati personali completi, o qualora sia necessario utilizzare immagini ai fini di ricerca, storici, addestramento interno o promozione dell'attività del Comando.

6. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, compresa la geolocalizzazione, in ragione delle particolari esigenze previste nel presente Regolamento, è limitata al massimo per 7 (sette) giorni dalla rilevazione. Sono fatte salve speciali esigenze di ulteriore conservazione nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria o di Polizia Giudiziaria.

In occasione di eccezionali e specifiche esigenze, il supervisore, per conto del titolare, potrà disporre la conservazione delle immagini per un periodo di tempo superiore, esplicitando documentata motivazione.

7. Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare, per configurazione, l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

8. Al termine della cessazione della necessità di trattamento, i dati personali devono essere distrutti.

Art. 11 - Utilizzo di particolari sistemi mobili

1. Per specifiche finalità concernenti la tutela della sicurezza e ordine pubblico, la prevenzione, l'accertamento e la repressione di reati, l'esecuzione di trattamenti ed accertamenti sanitari, la tutela della sicurezza e incolumità personali, gli operatori di Polizia Locale possono essere dotati di sistemi di telecamere personali o veicolari (*bodycam*, *dashcam*) per la ripresa di situazioni di criticità per la sicurezza propria o altrui.

Per le medesime finalità di tutela della sicurezza degli operatori e di gestione del personale sul territorio nell'espletamento dei compiti e mansioni di polizia locale, gli operatori possono essere dotati di dispositivi di geolocalizzazione.

2. Le videocamere e le relative schede di memoria ad uso personale di cui al comma precedente dovranno essere contraddistinte da un numero di identificazione e assegnate al singolo operatore, con atto o comunicazione informatica o telematica recante il giorno, l'orario, la qualifica e nominativo del

dipendente che, in caso di restituzione, invierà simile comunicazione di risposta. La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato. Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte al comma 1. Le *dashcam* possono operare in continuità, al fine della corretta ricostruzione della dinamica di eventuali sinistri. Eventuali altri simili strumenti di proprietà personale dovranno essere espressamente autorizzati da un responsabile del Corpo di Polizia Locale e dovranno essere adottate le identiche modalità descritte nel presente articolo. L'impiego della strumentazione sarà dettagliato in apposito disciplinare.

3. Il trattamento dei dati personali effettuati con simili sistemi di ripresa deve rispettare i principi di cui all'art. 5, RGDP ed, in particolare, i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati. In nessun caso potranno essere utilizzate le immagini ed i dati così raccolti per finalità di controllo dei lavoratori.

4. I sistemi di telecamere veicolari di cui al comma 1 potranno essere attivati in connessione all'avvio del veicolo sui quali sono installati. Dovranno essere configurati di *default* in sovrascrittura (*loop*). Non dovranno essere visualizzate o rimosse o salvate immagini e video o comunque non è ammesso l'accesso a tali dati se non per le finalità di cui al presente articolo e secondo i principi di cui all'art. 5 GDPR.

5. L'utilizzo degli impianti di videosorveglianza potrà essere attuato anche con la collaborazione di ausiliari di polizia giudiziaria appositamente incaricati per specifiche e limitate missioni. In particolare, i sistemi APR potranno essere utilizzati da ausiliari certificati per il pilotaggio, secondo la normativa vigente.

6. Possono essere utilizzate telecamere mobili, riposizionabili, anche del tipo foto-video-trappola. Qualora non sussistano necessità di indagine previste dal D.lgs 51/2018 e dalle specifiche norme procedurali che esimano il titolare del trattamento dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori delle aree interessate.

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, compatibilmente con i fini investigativi a tutela dell'ordine e sicurezza pubblica, prevenzione accertamento o repressione di reati, ex D.Lgs. 51/2018, ha diritto:

- a) di ottenere, dal titolare del trattamento, 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;

e) di esercitare gli ulteriori diritti previsti dalla normativa vigente e non espressamente sopra richiamati.

2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al supervisore o al titolare del trattamento dei dati. È considerata sempre la possibilità di coinvolgere il responsabile della protezione dei dati.

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 loro diritti, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sito istituzionale dell'Ente).

3. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare, a scopo esemplificativo, indicativamente:

- le proprie generalità complete e i recapiti di contatto;
- il luogo, la data e la fascia oraria della possibile ripresa, in un arco temporale strettamente limitato;
- 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 supervisore, il responsabile del trattamento o il diverso soggetto autorizzato dagli stessi, 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 *files* 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 di cui al comma 1 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. Qualora non sia possibile identificare l'interessato (o in caso di richieste eccessive o manifestamente infondate o di opposizione di un controinteressato) il supervisore, il responsabile del trattamento o il diverso soggetto designato dagli stessi, previa adeguata motivazione, informerà l'interessato dell'impossibilità di dare seguito alla richiesta;

9. Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

CAPO IV- MISURE DI SICUREZZA E ACCESSO

Art. 13 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente art. 10.

2. I dati raccolti mediante i sistemi di videosorveglianza e geolocalizzazione 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 mitigazione del rischio di leggibilità dei dati contenuti in schede, memorie e altri sistemi di archiviazione in caso di smarrimento degli stessi;

d) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, anche attraverso *audit* interni ed esterni.

3. Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, il titolare del trattamento, anche a mezzo del supervisore, 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 modulata e graduata la possibilità, per i diversi soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime immagini operazioni di cancellazione, di duplicazione o di oscuramento di parte delle riprese;

c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 10, 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*);
- g) gli accessi dovranno essere configurati di default in modo da garantire una disconnessione automatica dal sistema dopo un tempo preimpostato, per impedire l'accesso abusivo da parte di altri soggetti diversi dall'accedente.

5. Il titolare, il supervisore ed i responsabili del trattamento dei dati 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 e geolocalizzazione di cui al presente Regolamento sono custoditi presso il Comando di Polizia Locale di Gallarate, nonché presso le altre sedi e *data-center* collegate.
2. L'accesso alle centrali di controllo è consentito esclusivamente al titolare, al supervisore ed ai responsabili e altri soggetti autorizzati con specifico atto scritto dal titolare del trattamento o dal supervisore. I locali ove sono contenuti i *server* dovranno rimanere chiusi.
3. L'accesso alle centrali di controllo può essere consentito al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, sotto la vigilanza dei soggetti di cui al comma 2.
4. I responsabili impartiscono idonee istruzioni atte ad evitare modifiche, distruzioni, 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.

Art. 15 – Accesso agli impianti e ai dati

1. 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 di cui all'art. 3 del presente Regolamento.
2. Per finalità di indagine, l'Autorità giudiziaria e la polizia giudiziaria possono acquisire copia delle riprese in formato digitale, formulando specifica richiesta da conservare agli atti. Non è consentito fornire direttamente ai cittadini copia delle immagini.
3. Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, i filmati possono essere richiesti ed acquisiti dall'organo di polizia stradale che ha proceduto ai rilievi ed in capo al quale è posta l'istruttoria relativa alla dinamica dell'evento.

4. Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini o dell'imputato, a norma dell'art. 391-*quater* c.p.p., può richiedere copia digitale dei filmati presentando specifica richiesta scritta da conservare agli atti.

5. Il cittadino vittima o testimone di reato o il soggetto coinvolto in incidente stradale in cui non vi è stato intervento immediato di un organo di polizia stradale, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, o di richiedere intervento di un organo di polizia stradale, può richiedere al/ai soggetti designati del trattamento, quali responsabili del procedimento, che i filmati siano estratti e conservati cautelativamente oltre il termine di cui all'art. 10 del presente Regolamento, per essere messi a disposizione dell'organo di polizia o dell'A.G. procedente.

La richiesta deve pervenire entro il termine di 72 ore dall'evento, per consentire il salvataggio delle immagini da parte degli autorizzati al trattamento entro il termine massimo di conservazione.

L'organo di polizia o l'A.G. procedente formulano poi formale richiesta di acquisizione dei filmati entro tre mesi dall'evento, termine oltre il quale i dati non verranno conservati e dovranno essere cancellati.

6. In caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dell'estrazione delle immagini, nominativamente individuato per la gestione del procedimento, lascia traccia delle operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, in modo da garantire la genuinità dei dati stessi, annotando le operazioni compiute in apposito registro digitale.

7. In caso di richiesta ex commi 4 e 5 del presente articolo, l'istante dovrà effettuare il pagamento per le spese relative alle operazioni di analisi, estrazione, conservazione e archiviazione delle immagini, anche qualora dall'analisi delle immagini stesse non vi siano elementi ritenuti utili per le finalità per le quali abbia presentato istanza. Gli importi sono annualmente determinati dall'Ente.

8. L'accesso alle immagini necessario per curare o per difendere gli interessi giuridici del richiedente come sopra indicati è effettuato garantendo l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

9. Se l'accesso è effettuato, per le finalità ammesse dall'art. 3 del presente Regolamento ed in conformità a quanto previsto dal presente articolo, da personale del Corpo, l'istanza è sostituita da una richiesta annotata nel registro delle operazioni.

CAPO V- SISTEMI INTEGRATI DI VIDEOSORVEGLIANZA TRA PUBBLICO E PRIVATO

Art. 16 - Sistema integrato di videosorveglianza

1. Al fine di promuovere la sicurezza integrata sul territorio, recependo i contenuti del decreto legge 14/2017 convertito in legge 48/2017 "*Disposizioni urgenti in materia di sicurezza delle città*" e, in particolare, rispetto alle previsioni di cui all'art. 7 dello stesso, possono essere individuati specifici obiettivi per incrementare il controllo del territorio attraverso il concorso, sotto il profilo di sostegno strumentale, finanziario e logistico, di soggetti pubblici e privati. Tali obiettivi sono individuati nell'ambito dei "*Patti per l'attuazione della Sicurezza Urbana*" di cui all'art. 5 del predetto decreto, nel rispetto delle linee guida adottate.

2. Oltre all'ipotesi di cui al comma precedente, potranno essere attivate le seguenti tipologie di sistemi integrati, previa sottoscrizione di un protocollo di gestione:

- a) gestione coordinata di funzioni e servizi tramite condivisione delle immagini riprese da parte di diversi e autonomi Enti pubblici titolari del trattamento, utilizzanti le medesime infrastrutture tecnologiche;
- b) collegamento telematico di diversi titolari di trattamento ad un "centro" unico gestito da soggetto terzo;
- c) collegamento del sistema di videosorveglianza con la sala operativa di organi di polizia;
- d) collegamento al sistema di videosorveglianza di impianti privati il cui accesso è riservato esclusivamente ai soggetti dell'Ente previsti dal presente Regolamento.

Art. 17 - Partenariato pubblico privato per il potenziamento della videosorveglianza ad uso pubblico

1. Il Comune di Gallarate promuove ed attua, per la parte di competenza, il coinvolgimento dei privati per la realizzazione di singoli punti di videosorveglianza, orientati comunque su vie ed aree di pubblica disponibilità, nel rispetto dei principi di cui al presente Regolamento.

2. I privati interessati assumono su di sé ogni onere per:

- acquistare le attrezzature e renderle operative, con connessione al sistema centrale ovvero con memorizzazione locale delle immagini in conformità alle caratteristiche tecniche dell'impianto comunale o di un modello compatibile e metterle a disposizione del Comune a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa, assicurando che non si verifichino fenomeni di *lock-in*;
- effettuare la manutenzione su tali impianti.

3. Il Comune, unico abilitato alla visione, registrazione e salvataggio delle immagini, assume su di sé gli oneri per la gestione dei dati raccolti.

4. In accordo con il Comune e mediante la stipula di apposita convenzione - disciplinare, i soggetti privati che hanno ceduto i propri impianti di videosorveglianza al Comune potranno decidere di affidare il controllo diretto delle telecamere a istituti di vigilanza privata anche prevedendo l'installazione dell'impianto presso una sala di controllo dedicata collegata con la Centrale Operativa della Polizia Locale. Gli oneri finanziari dell'affidamento di tale servizio ricadranno sul soggetto privato, il quale, una volta individuato l'istituto di vigilanza privata a cui affidare il servizio, ne comunicherà il nominativo al Comune. Quale titolare del trattamento, il Comune impartirà le istruzioni affinché il trattamento avvenga nel rispetto delle norme a tutela dei diritti delle persone fisiche con riguardo ai dati personali.

5. Spetterà al Comune, in qualità di titolare del trattamento dei dati derivanti dal sistema di videosorveglianza, o, per conto del titolare, al Dirigente Comandante la Polizia Locale, procedere ai sensi di legge a tutti gli atti conseguenti, alla nomina del responsabile del trattamento dati e al conferimento dei compiti e dei ruoli necessari allo svolgimento del servizio ai singoli operatori dell'istituto di videosorveglianza individuati.

CAPO VI- TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 18 - Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

1. Per tutto quanto attiene il 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 ss., RGPD ed alle disposizioni attuative.

Art. 19 - 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 illecito 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, il supervisore 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 VII - DISPOSIZIONI FINALI

Art. 20 - Entrata in vigore

1. Il presente regolamento entra in vigore decorsi 15 (quindici) giorni dalla data di pubblicazione all'albo pretorio da effettuarsi dopo che la deliberazione di approvazione è divenuta esecutiva.

2. Dalla stessa data è abrogata ogni precedente normativa comunale in materia.

3. Copia del presente regolamento è pubblicata nell'apposita sezione del sito istituzionale.