N. 99

Comune di Triuggio

Provincia di Monza e Brianza

REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO TRAMITE DISPOSITIVI DI ACQUISIZIONE IMMAGINI E GEOLOCALIZZAZIONE

COMUNE DI TRIUGGIO

Approvato con deliberazione C.C. n. 47 del 22/11/2021

Sommario

CAPO I – DISPOSIZIONI GENERALI

1. Oggetto del Regolamento

Le immagini o la geolocalizzazione, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi detti sistemi incidono sul diritto delle persone alla propria riservatezza.

Il presente Regolamento disciplina le modalità di raccolta, gestione e conservazione dei dati personali mediante sistemi di videosorveglianza e geolocalizzazione ed in generale ogni trattamento dei dati personali effettuato mediante sistemi di acquisizione, registrazione, conservazione e gestione di immagini, audio-immagini, videoriprese e informazioni relative ad esse o alla localizzazione geografica e riguardanti le persone fisiche coinvolte, svolto in forma diretta o indiretta, dal Comune di Triuggio.

Il presente Regolamento garantisce altresì che lo stesso si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

In particolare, il presente regolamento:

a) definisce le modalità di utilizzo degli impianti di acquisizione immagini, videoriprese e informazioni ad esse relative (es. dati anagrafici, targhe, geolocalizzazione);

b) disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti.

2. Definizioni

Ai fini del presente Regolamento si intende:

1) Sistema di Videosorveglianza: è un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione e in generale l'utilizzo di immagini e videoriprese relative a persone fisiche identificate o identificabili, anche indirettamente.
2) Sistema di Geolocalizzazione è un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione e in generale l'utilizzo di informazioni sulla localizzazione geografica relative a persone fisiche identificate o identificabili, anche indirettamente.
3) Codice: è il D. Lgs. 196/2003, "Codice in materia di protezione dei dati personali".
4) RGPD: acronimo di "Regolamento Generale di Protezione del Dati" - è il Regolamento UE 2016/679 relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE".
5) Titolare del trattamento: secondo l'art. 4 del RGPD è "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". Nel contesto di questo Regolamento, il Titolare è il Comune di Triuggio (di seguito anche semplicemente "Ente").

6) Supervisore: è il soggetto (o più soggetti), designato dal Titolare, che sovrintende l'utilizzo di un sistema di gestione delle informazioni, coordinando le attività dei soggetti autorizzati al trattamento dei dati.
7) Responsabile della Protezione dei Dati: è una figura prevista dall'art. 37 del Regolamento UE 2016/679. Si tratta di un soggetto designato dal Titolare per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento);
8) Interessato: la persona fisica cui si riferiscono i dati personali oggetto di trattamento.

Ai fini delle definizioni di cui al presente Regolamento si deve fare riferimento all'art. 4 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e all'art 2 del D. lgs 51/2018 relativo 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.

3. Norme e linee guida di riferimento

Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto da:

- Regolamento UE Generale sulla Protezione dei Dati 2016/679 relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" e successive modifiche;
- 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";
- Decreto Legislativo 18 maggio 2018, n. 51, "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";

- DPR del 15/01/2018, n. 15, 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), nonché il provvedimento a carattere generale 29.11.2000, il decalogo delle regole per non violare la privacy ed il provvedimento a carattere generale 29.04.2004;
- Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivo video adottato il 29 gennaio 2020 dal Comitato Europeo per la protezione dei dati;
- Legge 20 maggio 1970, n. 300;
- Ispettorato nazionale del lavoro, circolare n. 2/2016 del 7.11.2016

4. Ambito di applicazione

Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali effettuati tramite sistemi di acquisizione e gestione immagini, audio e videoriprese e informazioni sulla geolocalizzazione geografica, svolti sotto la diretta titolarità del Comune di Triuggio e/o da altri soggetti in contitolarità con il Titolare, all'interno del territorio del Comune di Triuggio (ed eventualmente degli altri enti con esso convenzionati).

5. Principi generali

Il trattamento di acquisizione immagini, videoriprese e informazioni sulla geolocalizzazione all'interno dell'ambito precedentemente definito si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 del RGDP e, in particolare:

- **Principio di liceità** – Il trattamento di dati personali per mezzo di sistemi di videosorveglianza e geolocalizzazione 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) del RGPD. I trattamenti oggetto del presente Regolamento rispondono a detto principio e pertanto sono autorizzati 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) del RGPD, i sistemi di acquisizione immagini e videoriprese, 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 nei sistemi di videosorveglianza è escluso ogni uso superfluo e sono evitati eccessi e ridondanze.

- **Principio di proporzionalità** – La raccolta e l'uso delle immagini devono essere proporzionati 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. A tal riguardo si dà atto che detta valutazione di proporzionalità è stata effettuata dall'Ente su tutto il territorio comunale e che gli impianti di videosorveglianza, laddove previsti, sono stati adottati in quanto altre misure siano state previamente e ponderatamente valutate insufficienti o inattuabili (es. controlli da parte di addetti di Polizia Locale, posti di blocco, sistemi di allarme, misure di protezione degli ingressi) per il raggiungimento delle finalità indicate. In ogni caso l'Ente garantisce che il trattamento viene effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da controllare e/o da proteggere.
- **Principio di finalità** – Ai sensi dell'art. 5, paragrafo 1, lett. b) del RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana.

6. Finalità del trattamento e base giuridica

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

Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:

- Tutela della sicurezza urbana nei luoghi pubblici o aperti al pubblico;
- Tutela dell'integrità fisica della popolazione in occasione di eventi calamitosi;
- Tutela della sicurezza stradale, per monitorare la circolazione lungo le strade del territorio comunale e rilevare le infrazioni nonché fornire ausilio in materia di polizia amministrativa in generale;
- Registrazione di sedute consiliari per assicurare alla cittadinanza pubblicità, trasparenza e massima diffusione sulle attività dell'Ente;
- Tutela del patrimonio comunale, per presidiare gli accessi agli edifici comunali, dall'interno o dall'esterno, e le aree adiacenti o pertinenti ad uffici od immobili comunali;
- Tutela ambientale e rilevazione infrazioni;
- All'esigenza, unicamente in qualità di polizia giudiziaria, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali a norma del D. Lgs. 51/2018.

L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre forze di polizia e/o sicurezza, dovrà essere specificamente disciplinato con appositi accordi secondo la vigente normativa.

A tal riguardo l'Ente potrà altresì promuovere politiche di controllo del territorio integrate con organi istituzionalmente preposti alla tutela della sicurezza e dell'ordine pubblico. Dette politiche di controllo integrato e/o di collaborazione con altri Corpi o Organi preposti alla tutela della sicurezza e dell'ordine pubblico, anche al fine di consentire la visualizzazione diretta delle immagini degli apparati di videosorveglianza, vengono previamente disciplinati con separati accordi in forma scritta.

Si rimanda all'art. 31 del presente Regolamento per la modalità di definizione delle specifiche finalità di ogni impianto installato presso il territorio su cui tale regolamento viene applicato.

CAPO II – MODALITA' DI TRATTAMENTO DEI DATI

7. Acquisizione dei dati

I dati sono acquisiti tramite strumenti idonei al perseguimento delle finalità del Titolare, attraverso memorizzazione su specifici supporti installati sulle periferiche di acquisizione o trasmissione verso una centrale di acquisizione dei dati.

I sistemi di acquisizione di immagini e video sono installati in siti predefiniti dal Supervisore competente e tramite specifico atto di determinazione.

Il Supervisore competente definisce il numero e la tipologia di apparati di geolocalizzazione utilizzati in conformità con la propria autonomia organizzativa ed esigenza.

In ogni caso, le modalità di trattamento e di conservazione dovranno rispettare quanto disposto dalla vigente normativa, ed in particolare i dati personali oggetto di trattamento dovranno 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.

8. Trattamento da parte degli operatori

I dati acquisiti sono trattati da soggetti per cui sono stati definiti specifici profili di accesso, tra cui si possono prevedere:

- Visione delle immagini e delle videoriprese acquisite in tempo reale o da remoto;
- Consultazione istantanea della posizione geografica degli strumenti di geolocalizzazione, anche attraverso strumenti di rappresentazione su mappe digitali;
- Estrazione dei percorsi effettuati dagli strumenti di geolocalizzazione, eventualmente in forma anonima;
- Consultazione dei dati registrati;
- Gestione dei dati acquisiti, tra cui cancellazione, estrazione di copia su supporti digitali e/o stampa su supporti analogici;
- Svolgimento di operazioni avanzate sui sistemi di acquisizione, tra cui lo spegnimento/riavvio, il blocco, l'attivazione, lo zoom, il brandeggio, il riversamento delle immagini acquisite e l'utilizzo di funzionalità evolute.

I soggetti abilitati sono debitamente autorizzati al trattamento dei dati ed istruiti per il corretto utilizzo degli strumenti e dei supporti di memorizzazione dei dati.

I dati personali oggetto di trattamento, effettuato con strumenti elettronici nel rispetto delle misure di sicurezza indicate dalla normativa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per le finalità indicate nel presente Regolamento e resi utilizzabili per operazioni compatibili con tali scopi;

c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;

9. Estrazione di copia

E' consentita l'estrazione di copia dei dati acquisiti, nonché il riversamento su supporto digitale o analogico, ai fini della difesa di un diritto o del riscontro ad un'istanza di accesso, per assistere la competente autorità giudiziaria o di polizia giudiziaria o per rilevare infrazioni.

Tali attività possono essere svolte esclusivamente da soggetti appositamente autorizzati al trattamento.

I supporti digitali o analogici su cui vengono riversati i dati devono essere custoditi in sicurezza.

10. Comunicazione a terzi

Ove dovessero essere rilevate informazioni identificative di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, il Supervisore del sistema che ha acquisito i dati o un soggetto debitamente autorizzato provvederà a darne immediata comunicazione agli organi competenti.

Solo gli organi di Polizia e l'Autorità Giudiziaria potranno accedere alle informazioni raccolte, tramite consultazione presso le sedi del Titolare, trasmissione telematica o consegna di copia su supporto digitale o analogico

I sistemi di gestione potranno essere utilizzati anche a supporto di indagini di Autorità Giudiziaria, di organi di Polizia o di Polizia Locale.

Nel caso in cui gli organi della Polizia dello Stato o della Polizia Locale, ed in generale gli organi deputati alla pubblica sicurezza, nello svolgimento di loro indagini e/o altre attività, necessitino di disporre di informazioni ad esse collegate che sono contenute nei dati acquisiti, potranno farne richiesta scritta e motivata indirizzata al Supervisore sottoscritta dal richiedente e previa identificazione.

Ogni attività effettuata deve essere tracciata

11. Conservazione dei dati

I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conservati per il tempo necessario al perseguimento delle finalità perseguite ed in ogni caso entro i termini previsti dalla legge. Qualora, e solo per diverse comprovate esigenze, documentate caso per caso e rispondenti alle finalità istituzionali perseguite dall'Ente, sia necessario prolungare i termini di conservazione, deve esserne rilasciata ampia motivazione. Detta documentazione, a giustificazione di un termine di conservazione più lungo, deve essere conservata. Decorso il periodo di conservazione prestabilito, i dati registrati sono cancellati con modalità specificamente determinate a seconda del sistema di videosorveglianza.

Nel caso di acquisizione di dati di geolocalizzazione, i tempi di conservazione saranno predeterminati a seconda delle necessità di carattere organizzativo che hanno motivato l'utilizzo di tali strumenti e sino al raggiungimento delle finalità prefissate, nel rispetto dei termini di legge, salvo e solo per diverse comprovate esigenze, motivate e documentate, ed adottando idonee misure a tutela degli interessati. Decorso tale periodo, i dati registrati sono cancellati con modalità specificamente determinate a seconda del sistema di georeferenziazione. Considerato il rispetto dei principi di necessità e proporzionalità, l'esigenza di adottare un tempo superiore di conservazione dovrà essere valutato caso per caso e l'analisi e le considerazioni a supporto dovranno essere debitamente documentate.

La conservazione dei dati personali per un periodo di tempo superiore a quelli indicati precedentemente è ammessa altresì su specifica richiesta dell'Autorità Giudiziaria o di Polizia Giudiziaria, in relazione ad un'attività investigativa, ispettiva o repressiva in corso. In tali casi dovrà essere informato il Supervisore competente, che darà esplicite disposizioni ai soggetti designati ad operare per tale fine.

Per situazioni non rientranti nei casi analizzati precedentemente, la conservazione dei dati personali per un tempo eccedente a quanto stabilito è sempre subordinata ad una verifica preliminare di legittimità e necessità, il cui esito deve essere ampiamente documentato ed archiviato, a giustificazione della deroga temporale.

La conservazione dei dati deve essere effettuata nel rispetto delle misure di sicurezza previste dalla normativa vigente.

12. Cessazione del trattamento

In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali possono essere:

a) distrutti;

b) ceduti ad altro Titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti e se previsto da norme di legge o di regolamento;

c) conservati su richiesta di un'Autorità, per legge e a fini esclusivamente istituzionali.

La cessazione di trattamenti di dati in ogni caso deve essere conforme alle disposizioni del Regolamento UE 2016/679.

13. Accesso ai filmati

Al di fuori dei diritti dell'interessato e di quanto specificato nell'art. 20 del presente Regolamento, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente.

Ogni richiesta dovrà essere indirizzata al Supervisore designato.

Non è consentito fornire direttamente ai cittadini copia delle immagini.

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 e in capo al quale è l'istruttoria relativa all'incidente.

Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'Art. 391-quater c.p.p., può acquisire copia digitale dei filmati della videosorveglianza presentando specifica richiesta al Supervisore. In tal caso il difensore potrà presentare la richiesta motivata e provvedere alle spese per il

rilascio di copia digitale dei filmati della videosorveglianza, riversato su apposito supporto. Salvo l'ipotesi di conservazione per diverse finalità, i dati si intendono disponibili per i normali tempi di conservazione.

Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al Supervisore che i filmati siano conservati oltre i termini di Legge, per essere messi a disposizione dell'organo di polizia procedente. La richiesta deve comunque pervenire entro i termini di conservazione previsti. Spetterà all'organo di polizia in questione procedere a formale richiesta di acquisizione dei filmati.

In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal Supervisore dovrà tenere traccia delle operazioni eseguite.

CAPO III – SOGGETTI COINVOLTI NEI TRATTAMENTI

14. Titolare del trattamento

Il Comune di Triuggio è Titolare del trattamento dei dati personali acquisiti mediante utilizzo degli impianti di cui al presente Regolamento. A tal fine il Titolare è rappresentato dal Sindaco pro tempore, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.

Il Sindaco, in qualità di rappresentante del Titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti:

a) definisce le linee organizzative per l'applicazione della normativa di settore, confrontandosi direttamente con il Responsabile della Protezione dei Dati o interpellandolo per le questioni di competenza di quest'ultimo;

b) dispone le 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;

c) dispone quando necessario la valutazione di impatto sulla protezione dei dati di cui all'art. 35 del RGPD ed eventualmente la consultazione preventiva al Garante per la protezione dei dati personali di cui all'art. 36 RGPD, oltre a qualsiasi altra consultazione ritenuta necessaria per il corretto trattamento dei dati, interagendo con l'autorità nei casi previsti dalla norma;

d) designa i Supervisori del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di cui al presente regolamento, impartendo istruzioni ed assegnando compiti e responsabilità;

e) detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti;

f) vigila sulla puntuale osservanza delle disposizioni impartite

15. Supervisori del trattamento

Il Comandante Responsabile del Settore Polizia Locale del Comune di Triuggio o un diverso soggetto individuato dal Sindaco, è designato quale Supervisore del trattamento di dati personali effettuato mediante l'utilizzo degli impianti di cui al presente regolamento. La nomina è effettuata con atto del Sindaco, nel quale sono analiticamente specificati i compiti affidati. In particolare, il Supervisore:

a) individua e autorizza con propri atti i soggetti autorizzati al trattamento, definendo specificamente ruoli e responsabilità ed impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati; il Supervisore è responsabile dell'opportuna istruzione e formazione dei soggetti autorizzati, 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;

b) quando un trattamento deve essere effettuato da soggetti esterni per conto del Titolare del trattamento, il Supervisore ricorre a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato. Il ricorso a responsabili è disciplinato da un contratto o altro atto giuridico a norma, ai sensi dell'art. 28 RGPD;

c) provvede a rendere disponibile l'informativa "minima" e "di secondo livello" agli interessati secondo quanto definito all'art. 24 del presente Regolamento;

d) verifica e controlla che il trattamento dei dati effettuato mediante i sistemi di cui al presente regolamento, 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;

e) assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

f) 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, il Supervisore ha la responsabilità dell'adozione di tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;

g) 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;

h) 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;

i) 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;

l) 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;

m) assiste il Titolare nelle eventuali procedure di rilevazione di incidenti e 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;

n) supporta il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD 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;

o) 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;

p) assiste il Titolare nell'individuazione dei siti per cui si rende necessario il ricorso all'utilizzo di sistemi di videosorveglianza e nella determinazione dei tempi di conservazione delle immagini, delle videoriprese e dei dati di geolocalizzazione;

q) 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;

r) 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;

s) 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;

t) 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, vigilando sul rispetto da parte degli stessi degli obblighi di corretta e lecita acquisizione ed utilizzazione dei dati e, in caso di violazione, segnalando le stesse al Titolare e procedendo alle contestazioni in forma scritta;

u) garantisce la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale autorizzato con riferimento ai trattamenti realizzati mediante gli impianti oggetto del presente regolamento, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali.

16. Soggetti autorizzati al trattamento dei dati personali

Il Supervisore del trattamento autorizza i soggetti al trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di cui al presente Regolamento. L'autorizzazione è formalizzata 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 tenendo conto della loro esperienza, capacità e affidabilità al fine di garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

In particolare, i soggetti autorizzati devono:

a) utilizzare sempre le proprie credenziali personali per l'accesso ai sistemi informatici, garantendone la riservatezza; i sistemi devono garantire la registrazione degli accessi ed il tracciamento;

b) mettere in sicurezza gli strumenti di accesso alle informazioni e gli eventuali supporti di memorizzazione assegnati, in modo da evitare che i dati trattati siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

c) mantenere la massima riservatezza sulle informazioni di cui vengano a conoscenza nell'esercizio delle loro mansioni;

d) custodire e controllare e conservare i dati personali rispettando le misure di sicurezza predisposte dall'Ente, 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) evitare di creare banche dati nuove senza autorizzazione espressa del Supervisore del trattamento;

f) segnalare al Supervisore situazioni per cui, nello svolgimento delle attività assegnate, dovessero venire a conoscenza di informazioni eccedenti la propria autorizzazione al trattamento, oppure dovessero ravvisare elementi che potrebbero inficiare la sicurezza dei sistemi, dei dati trattati o dei supporti di memorizzazione;

g) fornire al Supervisore 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;

h) garantire la massima collaborazione in caso di istanze avanzate da parte degli interessati, di accertamenti/ispezioni da parte dell'Autorità Garante per la protezione dei dati personali e di richieste di accesso ai dati da parte di autorità giudiziarie o di polizia giudiziaria, attenendosi alle disposizioni del Supervisore o del Titolare.

I soggetti autorizzati, a cui viene impartita apposita formazione, devono trattare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare o del Supervisore.

La gestione e l'utilizzo dei sistemi di videosorveglianza aventi per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è riservata agli organi di Polizia Locale, aventi qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del codice di procedura penale.

L'utilizzo dei dispositivi di acquisizione da parte dei soggetti autorizzati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato nonché alle specifiche istruzioni impartite.

In caso di sostituzione del Supervisore, persiste la validità delle autorizzazioni precedentemente attribuite, salvo che il nuovo Supervisore disponga diversamente; il nuovo Supervisore è comunque tenuto a verificare la sussistenza delle autorizzazioni precedentemente rilasciate, provvedendo al loro aggiornamento in caso di necessità.

17. Soggetti esterni che trattano dati per conto del Titolare

Il Titolare del trattamento, anche tramite il Supervisore, ha la facoltà di avvalersi di soggetti esterni, in qualità di responsabili, per lo svolgimento di attività correlate alla gestione e al funzionamento dei sistemi, che potrebbero comportare, seppur in maniera accidentale, un trattamento di dati.

Queste attività possono comprendere la manutenzione tecnica degli impianti, l'amministrazione dei sistemi informatici, il backup delle informazioni, la profilazione delle utenze che accedono ai dati, la conservazione presso proprie infrastrutture tecnologiche dei dati acquisiti e tutte le operazioni che potrebbero comportare, per loro natura, delle criticità in merito alla protezione dei dati personali.

I soggetti a cui il Titolare ricorre in qualità di responsabili devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato.

Il Titolare disciplina i trattamenti effettuati da parte del responsabile mediante contratto ovvero altro atto giuridico, specificando obblighi e responsabilità ai sensi degli artt. 28 e 29, RGPD. La regolamentazione di tali impegni può essere formalizzata dal Supervisore o altri soggetti designati.

Il Supervisore aggiorna periodicamente la lista dei responsabili esterni del trattamento.

18. Amministratori di Sistema

Tra le mansioni assegnate ai soggetti autorizzati o ai responsabili esterni possono rientrare attività tecniche di gestione e manutenzione di sistemi elaborativi o di loro componenti.

In tali casi, devono essere esplicitate per tali soggetti, interni o esterni, le mansioni di amministrazione dei sistemi assegnate con precisa definizione dei rispettivi perimetri operativi e responsabilità.

Coloro che svolgono mansioni di amministrazione dei sistemi informatici devono essere espressamente designati da soggetti aventi titolo di rappresentare il Titolare negli specifici contesti del trattamento.

Il Supervisore redige e mantiene aggiornato l'elenco degli amministratori di sistema designati fra il personale dell'Ente, oltre che l'elenco dei responsabili esterni che svolgono mansioni di amministrazione dei sistemi. Questi ultimi, a loro volta, sono tenuti a mantenere aggiornato l'elenco delle persone fisiche che operano come amministratori di sistema per conto del Titolare, che dovrà essere reso disponibile su richiesta dell'Ente.

Il Supervisore e i responsabili sono tenuti, per i contesti di loro competenza e responsabilità, al rispetto delle prescrizioni specificate nel provvedimento del Garante Privacy sugli amministratori di sistema e aggiornamenti successivi.

CAPO IV – MISURE DI SICUREZZA

19. Accesso fisico ai sistemi e ai luoghi

I dati personali acquisiti mediante l'utilizzo dei sistemi di videosorveglianza di cui al presente Regolamento sono custoditi in modalità criptata in zone ad accesso riservato.

In caso di locali interni all'Ente l'accesso è consentito esclusivamente al Titolare, al Supervisore competente, ai soggetti autorizzati e ai responsabili, individuati ai sensi degli articoli 15, 16, 17 del presente Regolamento. L'accesso da parte di soggetti diversi da quelli precedentemente indicati è subordinato al rilascio, da parte del Titolare o del Supervisore, 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 dal Supervisore. L'accesso ai locali può essere consentito esclusivamente ad incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità definite per lo specifico trattamento di dati, nonché al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali.

Il Supervisore competente impartisce 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.

I soggetti autorizzati vigilano sulla puntuale osservanza delle istruzioni impartite dal Supervisore e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

In caso i dati personali siano custoditi in siti esterni a seguito di specifica prestazione di servizio conferita ad un responsabile esterno, quest'ultimo è tenuto a garantire

l'adozione di adeguate misure di sicurezza fisica al fine di ridurre al minimo il rischio di accesso non autorizzato ai sistemi e ai luoghi presso cui viene effettuato il trattamento.

20. Accesso logico ai sistemi e ai dati

L'accesso ai sistemi che gestiscono i dati oggetto del presente regolamento e ai dati oggetto dello specifico trattamento può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate su disposizione del Supervisore del trattamento.

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 perseguimento delle finalità definite per lo specifico trattamento di dati.

L'accesso ai dati è consentito esclusivamente:

a) al Titolare, al Supervisore ed ai soggetti autorizzati al 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 dal Pubblico Ministero e acquisita dall'Ente);

c) ai responsabili incaricati della manutenzione dei sistemi, nei limiti strettamente necessari alle specifiche esigenze di funzionamento dell'impianto medesimo ovvero, in casi del tutto eccezionali, agli amministratori di sistema dell'ente specificamente designati per tale contesto (preventivamente autorizzati al trattamento dei dati);

d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso, previo accoglimento della relativa richiesta laddove ne sussistano i presupposti. L'accesso da parte dell'interessato sarà limitato ai soli dati che lo riguardano direttamente; al fine di evitare l'accesso ad informazioni riguardanti altri soggetti, dovranno pertanto essere utilizzati, da parte dell'Ente, adeguati accorgimenti tecnici 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 ai dati sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante 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;

f) agli altri enti e/o organi di sicurezza pubblica, previo accordo scritto, ed agli altri casi specificamente previsti al precedente articolo 13, come disposto dal presente regolamento.

21. Sicurezza nelle trasmissioni

La trasmissione attraverso reti pubbliche di comunicazioni di immagini, video e/o audio-riprese e dati di geolocalizzazione acquisite tramite dispositivi sarà effettuata previa applicazione di tecniche di cifratura che ne garantiscano la riservatezza.

I Supervisori sono tenuti a disporre l'adozione di adeguati sistemi di sicurezza per garantire la riservatezza delle trasmissioni telematiche nei contesti di propria competenza e responsabilità nonché garantire la separazione della rete di videosorveglianza da altre reti.

22. Ruoli, mansioni e responsabilità

I Supervisori, nell'ambito delle rispettive attività di gestione dei sistemi di videosorveglianza e coordinamento dei processi organizzativi, possono avvalersi dell'operato di soggetti autorizzati e di responsabili esterni attribuendo ad essi specifici ruoli, mansioni e responsabilità, fra cui:

a) accesso ai sistemi per la visualizzazione dei dati in tempo reale;

b) accesso ai sistemi per la consultazione dei dati registrati;

c) estrazione di copia dei dati in formato analogico e/o digitale e conversione in altri formati;

d) assegnazione di strumenti elettronici idonei per la consultazione dei dati;

e) attribuzione di specifici profili di accesso agli operatori;

f) riversamento di immagini e videoriprese acquisite tramite supporti di memorizzazione installati su dispositivi di acquisizione;

g) estrazione dei percorsi effettuati dagli strumenti di geolocalizzazione, eventualmente in forma anonima

h) utilizzo di funzionalità avanzate dei dispositivi in dotazione (es. zoom, brandeggio, ecc);

i) assegnazione di compiti manutentivi;

j) attribuzione di mansioni di configurazione di sistemi e/o rilascio di credenziali con relativi profili di accesso;

k) assegnazione di qualsiasi altro incarico necessario per il corretto trattamento dei dati.

Ogni specifica attribuzione di ruoli e responsabilità deve essere formalizzata e accompagnata da apposite istruzioni organizzative ed operative.

L'attribuzione di profili di accesso, di strumenti operativi nonché di funzioni correlate al trattamento di dati deve essere effettuata a seguito di valutazione dell'esperienza, capacità e affidabilità dei soggetti destinatari, e previa adeguata formazione, al fine di garantire l'adeguata sicurezza dei sistemi e dei dati.

23. Utilizzo degli strumenti e dei supporti di memorizzazione

I soggetti autorizzati sono tenuti a garantire la custodia in sicurezza degli strumenti utilizzati e dei supporti di memorizzazione impiegati, prestando la massima attenzione durante il loro impiego e riponendoli nei luoghi destinati alla loro conservazione, in modo da ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati.

Gli strumenti assegnati che consentano l'accesso ai dati devono essere protetti da sistemi di autenticazione, devono essere criptati e non devono essere lasciati incustoditi.

Qualora la presa in carico delle immagini e delle videoriprese venga effettuata tramite riversamento dai supporti di memoria presenti negli strumenti di acquisizione, i file contenenti dati devono essere rimossi dai supporti una volta acquisiti i dati.

In caso di dismissione di supporti di memorizzazione, questi devono essere resi inutilizzabili tramite danneggiamento fisico irreparabile, in modo che non sia consentito in alcun modo il recupero dei dati trattati.

CAPO V – OBBLIGHI DEL TITOLARE

24. Informativa

Gli interessati devono essere sempre informati del trattamento effettuato dal Titolare.

In particolare, nei casi di acquisizioni di immagini e videoriprese devono essere informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici.

A tal fine il Titolare utilizzerà una informativa cosiddetta di "primo" e di "secondo livello".

Quanto all'informativa di "primo livello", finalizzata per relazionarsi in modo primario e diretto con l'interessato, il Titolare utilizzerà un cartello di avvertimento per dare una visione di insieme del trattamento previsto in modo facilmente visibile, comprensibile e chiaramente leggibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno. Il cartello è posizionato prima di entrare nell'area monitorata. Detto cartello riporterà le informazioni più importanti, comprese quelle di maggior impatto per l'interessato (es. finalità e base giuridica del trattamento, identità del Titolare, i dati di contatto del Responsabile della Protezione dei Dati e i diritti degli interessati, il periodo di conservazione, le modalità di trasmissione). Verrà inoltre riportato anche il luogo ove l'interessato potrà prendere visione dell'informativa per esteso.

In presenza di più dispositivi di acquisizione, in relazione alla vastità dell'area e alle modalità delle riprese, potranno essere installati più cartelli informativi.

Il cartello potrà inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificato al fine di informare se le immagini sono solo visionate o anche registrate.

Quanto all'informativa di "secondo livello", essa verrà resa disponibile in luogo facilmente accessibile all'interessato, come il sito istituzionale dell'Ente, e dovrà contenere tutte le informazioni obbligatorie previste dall'art. 13 RGPD. Nel medesimo luogo sarà resa disponibile altresì la geo-localizzazione delle telecamere presenti sul territorio comunale.

L'Ente, nella persona del Supervisore, si obbliga ad informare preventivamente la comunità cittadina dell'avvio del trattamento dei dati personali effettuato tramite l'impianto di videosorveglianza, anche attraverso una sua mappatura, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale, tra cui il portale istituzionale.

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.

Nel caso in cui il trattamento preveda la sorveglianza di una zona di ampia dimensione, si provvederà ad informare i soggetti interessati tramite apposita diffusione sul sito istituzionale della zona soggetta al trattamento.

In caso di acquisizione di dati di geolocalizzazione, il Titolare dovrà fornire agli interessati un'informativa comprensiva di tutti gli elementi contenuti nell'art 13 del RGPD e dovrà apporre sui dispositivi e sui veicoli oggetto di geolocalizzazione un'adeguata informativa semplificata di facile comprensione.

25. Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, oltre alla dovuta informativa, l'interessato, dietro 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 nelle modalità previste dal presente Regolamento;

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 e di tutto quanto previsto ex art. 13 RGPD;

c) di richiedere la cancellazione nei casi previsti dal Regolamento UE 2016/679 qualora sussista uno dei motivi di cui all'art. 17 del RGPD, nonché 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, nei casi previsti dal Regolamento UE 2016/679, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21 del RGPD. Il Supervisore informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti.

e) L'interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'art. 18 del RGPD. In tali casi i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

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 del RGPD ovvero al Supervisore del trattamento designato dal Titolare, che, laddove necessario, si consulterà con il Responsabile della Protezione dei Dati.

Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare le informazioni utili alla sua identificazione tramite il sistema di videosorveglianza, fra cui il luogo, la data e la fascia oraria della possibile ripresa.

Il Supervisore 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, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della loro acquisizione, in ossequio alla previsione di cui all'art. 15, paragrafo 4 del RGPD.

Qualora il Supervisore non sia in grado di identificare l'interessato o in caso di richieste eccessive o manifestamente infondate da parte dell'interessato, il Supervisore – previa adeguata motivazione – informerà l'interessato dell'impossibilità di dare seguito alla richiesta.

In caso di richiesta di accesso ai dati di geolocalizzazione, l'interessato potrà chiedere di consultare tutti i dati che lo riguardano in possesso del Titolare, fornendo tutte le informazioni necessarie per determinare specificamente i contesti che lo riguardano, come gli strumenti e i veicoli utilizzati oltre che il periodo di utilizzo.

Qualora, ai sensi dell'art. 15, paragrafo 3 del RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files i dati in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della loro acquisizione, in ossequio alla previsione di cui all'art. 15, paragrafo 4 del RGPD.

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.

Nell'esercizio dei propri 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.

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.

26. Valutazione di impatto sulla protezione dei dati

In ossequio al disposto di cui all'art. 35 RGPD, qualora il trattamento di dati realizzato mediante i sistemi oggetto del presente regolamento possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare provvederà – previa consultazione con il Responsabile della Protezione dei Dati - all' effettuazione di una valutazione di impatto sulla protezione dei dati personali.

Il Titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

La valutazione di impatto non verrà effettuata qualora il trattamento dovesse rientrare nell'elenco delle tipologie di trattamenti, redatto dal Garante della Privacy, per le quali non è richiesta.

27. Utilizzo in ambienti di lavoro

Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300, gli impianti di videosorveglianza e gli strumenti di rilevazione di dati di geolocalizzazione non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'Ente, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Qualsiasi utilizzo di sistemi in ambienti di lavoro deve soddisfare i principi di liceità, non eccedenza e proporzionalità.

Il Titolare deve quindi attivarsi, in caso di necessità, per l'attuazione di misure di garanzia ai sensi dello Statuto dei Lavoratori.

CAPO VI – ALTRE DISPOSIZIONI

28. Sistemi integrati di trattamento dei dati

In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, previo accordo scritto con gli Organi interessati, è possibile il ricorso a sistemi integrati di trattamento dei dati tra diversi soggetti, pubblici e privati.

Nell´ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati:

a) gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, dei dati da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le

medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare i dati solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

b) collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 28 RGPD da parte di ogni singolo Titolare, deve assumere un ruolo di coordinamento e gestione dell' attività di trattamento senza consentire, tuttavia, forme di correlazione dei dati per conto di ciascun Titolare;

c) sia nelle predette ipotesi, sia nei casi in cui l'attività di trattamento venga effettuata da un solo Titolare, si può anche attivare un collegamento dei sistemi di gestione con le sale o le centrali operative degli organi di polizia. L' attivazione del predetto collegamento deve essere reso noto agli interessati.

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza, quali:

1) adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del Titolare, comunque non inferiore a sei mesi;

2) separazione logica dei dati registrati dai diversi titolari.

Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di trattamento abbiano natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il Titolare del trattamento può effettuare una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD.

29. Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

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 ss. del RGPD ed alle disposizioni attuative e dagli artt. 37 e ss. del D. lgs. 51/2018 relativo 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.

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

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 del RGPD.

Il Titolare e/o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

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 del RGPD.

31. Provvedimenti attuativi

Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi derivanti dal presente Regolamento, fra cui l'adozione di atti che descrivano nello specifico i trattamenti di dati effettuati dal Titolare e la definizione di ogni ulteriore e specifico elemento ritenuto utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento e dalle leggi ivi applicabili, ed entro i limiti da questi ultimi imposti.

Specifici disciplinari verranno redatti di concerto tra la Giunta e il Supervisore al fine di regolare nello specifico determinati trattamenti inerenti il sistema di videosorveglianza.

Previa istanza da parte del Supervisore, nonché in ottemperanza ed entro i limiti, il contesto e le modalità di quanto disposto dal presente Regolamento e dalle leggi ivi applicabili, spetterà altresì alla Giunta l'adozione di nuovi strumenti, sistemi e tecnologie integrativi all'attuale sistema di videosorveglianza (es. adozione di droni, dashcam, bodycam, fototrappole ecc.), unitamente al controllo sulla adeguatezza delle misure di sicurezza.

In seguito alle nuove adozioni, compete alla Giunta Comunale di provvedere ad aggiornare atti ed informazioni di cui al sistema di videosorveglianza.

Detti atti ed informazioni, ed i relativi disciplinari, andranno di volta in volta ad integrare il presente Regolamento, pur non facendone parte.

Sarà sempre onere della Giunta valutare le idonee garanzie e competenze offerte da tutti i fornitori coinvolti, nonché di chiedere alle ditte produttrici le specifiche delle tecnologie e dei sistemi utilizzati, ivi comprese le misure di sicurezza, che verranno individuate con apposita documentazione tecnica rilasciata dalla medesima Ditta produttrice, da conservare unitamente ai disciplinari adottati.

La Ditta produttrice dovrà fornire altresì le caratteristiche fisiche degli strumenti e la descrizione del loro funzionamento.

La valutazione effettuata dalla Giunta avrà sempre il fine di ridurre al minimo i rischi di violazione dei dati, ed in particolare di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati personali.

In seguito a nuove adozioni, rimane sempre in capo ai Supervisori l'onere di adottare appositi atti che prevedano:

- l'autorizzazione ai soggetti che tratteranno i dati, specificando per ognuno il perimetro di azione;

- la designazione dei responsabili del trattamento ai sensi dell'art. 28 RGPD che tratteranno i dati in nome e per conto del Titolare e la lista relativa al loro aggiornamento;

- la designazione degli Amministratori di Sistema, con specificazione degli ambiti di operatività;

- l'elenco dei siti in cui potranno essere collocati i sistemi di acquisizione delle immagini, sulla base delle necessità rilevate e in osservanza al principio di proporzionalità;

- l'eventuale introduzione di nuovi sistemi di geolocalizzazione, le cui caratteristiche di sicurezza siano compatibili con le prescrizioni della Giunta Comunale;

- l'attuazione di tutte le misure che garantiscano la sicurezza dei dati trattati e dei sistemi implementati.

- l'aggiornamento delle informative e della cartellonistica.

32. Modifiche regolamentari

I contenuti del presente regolamento dovranno essere aggiornati nei casi di revisione normativa in materia di trattamento dei dati personali e in materia di videosorveglianza. In ogni caso ogni modifica al presente Regolamento dovrà essere approvata da parte del Consiglio Comunale.

33. Entrata in vigore e norme di rinvio

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.

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

Per quanto non disciplinato dal presente Regolamento si rinvia al Codice della Privacy come modificato dal D. lgs 101/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, al Regolamento UE 2016/679 e al D. lgs 51/2018 relativo 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 ai provvedimenti generali sulla videosorveglianza approvati dall'Autorità garante per la protezione dei dati personali e alle indicazioni centrali dell'Anci e del Ministero dell'interno.

Il presente regolamento è stato approvato dal Consiglio Comunale con deliberazione n.47 del 22/11/2021.

L'avviso di deposito del suddetto regolamento è stato pubblicato all'albo pretorio dal 23/11/2021 al 08/12/2021.

Entrato in vigore il 1° gennaio 2022

Triuggio, 8 febbraio 2022

IL SEGRETARIO GENERALE
Dr. Salvatore Ferlisi