COMUNE DI ROBBIATE

Regolamento per l'esercizio del sistema di videosorveglianza comunale

30 Novembre 2020

Delibera C.C. n. xxxxx/xxxx

Sommario

PREMESSA....3
Art. 1 – Principi generali....5
Art. 2 - Definizioni....6
Art. 3 - Obiettivo del presente Regolamento....9
Art. 4 - Ambito di validità e di applicazione del presente regolamento....9
Art. 5 - Identificazione del titolare del trattamento dei dati....9
Art. 6 - Obiettivi e finalità del sistema di videosorveglianza....10
Art. 7 – Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità, e finalità....12
7.1 Premessa....12
7.2 Principio di liceità....12
7.3 Principio di necessità....13
7.4 Principio di non eccedenza e proporzionalità....14
7.5 Principio di finalità....14
Art. 8 – Utilizzi esplicitamente vietati....15
Art. 8 bis – Deposito di rifiuti....15
Art. 9 – Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada....16
Art. 10 - Utilizzo di particolari videocamere mobili....17
Art. 11 – Accordi con enti pubblici e privati....18
Art. 12 – Tipi di trattamenti autorizzati....18
Art. 13 – Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati....20
Art. 14 – Accesso ai dati da parte delle forze dell'ordine e dell'Autorità Giudiziaria....21
Art. 15 – Accesso telematico da parte di Carabinieri e Polizia di Stato....22
Art. 16 – Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento....22
Art. 17 – Designazione degli autorizzati del trattamento dei dati....22
Art. 18 – Obblighi degli autorizzati/operatori....22
Art. 19 – Tempi di conservazione delle immagini....23
Art. 20 – Cifratura dei dati trasmessi mediante apparati e tecnologie wireless....23
Art. 21 – Luogo e modalità di memorizzazione delle immagini....23
Art. 22 - Criteri e modalità di estrazione delle immagini....24
Art. 23 – Ottemperanza al Provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativo al controllo dell'operato degli amministratori di sistema....24

Art. 24 – Installazione di nuove telecamere 25
Art. 25 – Installazione di telecamere mobili 25
Art. 26 – Informativa 26
Art. 27 - Riscontro all'interessato 26
Art. 28 – Requisiti minimi sul luogo di collocazione del server 27
Art. 29 – Requisiti minimi sugli strumenti elettronici, informatici e telematici 28
Art. 30 – Cessazione del trattamento 28
Art. 31 – Limiti alla utilizzabilità dei dati personali 28
Art. 32 – Danni cagionati per effetto del trattamento dei dati personali 29
Art. 33 – Comunicazione 29
Art. 34 – Tutela amministrativa e giurisdizionale 30
Art. 35 – Modifiche e integrazioni regolamentari 30
Art. 36 – Norme finali 30
Art. 37 – Pubblicità e conoscibilità del regolamento 30

PREMESSA

Il presente regolamento è redatto a norma del:

1. Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati o GPDR);
2. Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
3. Decreto Legislativo 10 agosto 2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", che modifica e integra il dlgs 196/2003 Codice nazionale sulla privacy";
4. Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, "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";
5. Decreto Legislativo 18 maggio 2018, n. 51/2018 "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;

6. Provvedimento del Garante per la Protezione dei Dati personali in materia di videosorveglianza – 8 aprile 2010;

Art. 1 – Principi generali

1. Il presente regolamento garantisce che il trattamento di dati personali, effettuato mediante l'attivazione di un impianto di videosorveglianza gestito ed impiegato dai Comuni di **ROBBIATE (LC), PADERNO D'ADDA (LC), VERDERIO (LC),** si svolga nel pieno rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza ed alla identità personale.
2. E' stato stipulato un accordo di contitolarità ai sensi dell'art. 26 del regolamento europeo (EU) 2016/679 per la gestione dei trattamenti dati personali Gestione del servizio di Polizia Locale tra i tre enti.
3. La raccolta e l'uso delle immagini avviene con l'assoluta osservanza dei principi e dei limiti sanciti dal Regolamento Europeo RGDP 2016/679/UE e del D.L.gs 196/2003 del 30 giugno 2003 (Codice in materia di protezione dei dati personali) s.m.i. e nel pieno rispetto delle indicazioni dell'Autorità Garante della tutela dei dati personali contenute nel "Provvedimento Generale sulla Videosorveglianza" dell'8 aprile 2010 ed in particolare secondo i presupposti di:
   a. Liceità: il trattamento di dati personali attraverso l'impianto di videosorveglianza è aderente alle funzioni strettamente istituzionali dell'Ente di cui è investito il titolare del trattamento in ossequio al disposto di cui all'art. 6, paragrafo1, lettera e del RGDP. La videosorveglianza comunale, pertanto, è consentita senza necessità di consenso da parte degli interessati;
   b. Necessità: perché il sistema di videosorveglianza impiegato dall'Ente verrà configurato per l'utilizzazione al minimo dei dati personali e dei dati identificativi, in modo da evitare l'uso superfluo od eccessivo e ridondante di cui all'art. 5, paragrafo 1, lettera c) del RGDP. 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;
   c. Proporzionalità: la raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla

commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate in sufficienti 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 parti di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità di trattamento. Nell'uso delle apparecchiature volte a riprendere, per legittimi interessi indicati, aree esterne ad edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere.

d. Finalità: ai sensi dell'art. 5, paragrafo 1, lettera b) del RGDP, i dati particolari vengono raccolti per finalità determinate. E' consentito, pertanto, la videosorveglianza come misura volta a migliorare e garantire la sicurezza urbana.

Art. 2 - Definizioni

1. Ai fini del presente regolamento si intende per:
   a. **"banca dati"**: il complesso organizzato di dati personali, formatosi presso il Comando di Polizia Locale e trattato esclusivamente mediante riprese videoregistrate, in relazione ai luoghi di installazione delle telecamere, riguarda prevalentemente soggetti e i mezzi di trasporto che transitano nell'area interessata;
   b. **"trattamento di dati personali"**: qualunque operazione o complesso di operazioni, effettuati con l'ausilio di strumenti elettronici o comunque automatizzati, concernenti la raccolta, la immissione, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati**;**

c. **"dato personale"**: qualunque informazione relativa a persona fisica, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale e rilevati con trattamento di suoni ed immagini effettuati attraverso l'impianto di videosorveglianza;
d. **"dati identificativi"**: i dati personali che permettono l'identificazione diretta dell'interessato;
e. **"dato anonimo"**: il dato che in origine, a seguito di inquadratura o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
f. **"dato particolare"**: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, dati biometrici, dati genetici, dati giudiziari.
g. **"titolare del trattamento"**: i Comuni di Comuni di Robbiate, Paderno d'Adda, Verderio cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
h. **"responsabile del trattamento"**: la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento di dati personali
i. **"interessato"**: la persona fisica cui si riferiscono i dati personali;
j. **"autorizzati"**: le persone fisiche autorizzate dal titolare o dal responsabile, a compiere operazioni di trattamento di dati personali;
k. **"designato"**: L'art 2-quaterdecies del decreto legislativo 101/2018 ha introdotto la definizione di "soggetto designato", persona fisica espressamente designata che opera sotto l'autorità del Titolare o Responsabile
l. **"blocco"**: la conservazione di dati personali con sospensione temporanea di ogni altra operazione di mutamento;

m. **"comunicazione"**: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal responsabile e dagli autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n. **"diffusione"**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
o. **"videosorveglianza fissa"**: la sequenza di componenti e di apparati – di natura hardware e software – che costituiscono un sistema di videosorveglianza urbana basato sulla ripresa di immagini, suoni e dati che provengono da apparati di ripresa (TVCC) installati su supporti fissi (pali, sbracci, etc, etc);
p. **"videosorveglianza mobile"**: la sequenza di componenti e di apparati di natura hardware e software che costituiscono un sistema di videosorveglianza urbana basato sulla ripresa di immagini, suoni e dati, che provengono da apparati di ripresa (TVCC) installati su mezzi mobili (moto, autovetture, mezzi mobili attrezzati ed autorizzati allo scopo, etc, etc);
q. **"Codice Privacy"**: il Codice in materia di protezione dei dati personali approvato con D.L.gs 30 giugno 2003 n.196 e successive modifiche e integrazioni;
r. **"Garante privacy"**: Il Garante per la protezione di dati personali;
s. **"Regolamento Europeo"** regolamento (UE) n. 2016/679 e meglio noto con la sigla GDPR, è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018.

Art. 3 - Obiettivo del presente Regolamento

Obiettivo del presente regolamento è assicurare che i trattamenti di dati personali effettuati dai Comuni di Robbiate Paderno d'Adda Verderio nel proprio territorio mediante il sistema di videosorveglianza, avvengano correttamente, lecitamente, e conformemente a quanto previsto dalla disciplina rilevante in materia di sicurezza e protezione dei dati personali; in particolare, il rispetto del presente regolamento garantirà la conformità:

- alle prescrizioni del Regolamento (UE) n. 2016/679 in materia di protezione dei dati personali;
- alle prescrizioni del D.Lgs. 196/2003 s.m.i. (Codice in materia di protezione dei dati personali);
- ai provvedimenti del Garante per la protezione dei dati personali, con particolare riferimento al provvedimento generale del 8 aprile 2010 del Garante per la protezione dei dati personali, dedicato alla videosorveglianza; ai principi di: liceità; necessità; non eccedenza e proporzionalità; finalità.

Art. 4 - Ambito di validità e di applicazione del presente regolamento

Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali e particolari effettuati mediante sistema di videosorveglianza sotto la diretta titolarità dei Comuni di Robbiate Verderio e Paderno d'Adda, e all'interno del territorio degli stessi enti. L'impianto di videosorveglianza è descritto nell'Allegato n. A, che è parte integrante e sostanziale del presente regolamento.

Art. 5 - Identificazione del titolare del trattamento dei dati

I titolari dei trattamenti di dati personali effettuati mediante il sistema di videosorveglianza sono i Comuni di Robbiate, Paderno d'Adda, Verderio: pertanto, competono esclusivamente agli enti le decisioni in ordine alle finalità e alle modalità del trattamento, compreso anche il profilo della

sicurezza. A titolo esemplificativo e non esaustivo, si riportano di seguito alcune decisioni che spettano esclusivamente al Titolare:

- il numero, la tipologia e i luoghi di installazione attuale e futura delle telecamere;
- i tempi massimi e minimi di memorizzazione delle immagini;
- gli strumenti elettronici, informatici e telematici da utilizzare per la gestione delle immagini, compresa la ripresa e la memorizzazione delle immagini stesse;
- l'individuazione dei soggetti che possono essere a vario titolo coinvolti (in qualità di autorizzati, oppure di designati interni o responsabili oppure di autonomi titolari) nelle operazioni di trattamento dai dati e nelle operazioni di amministrazione di gestione di sistema informatico e telematico;
- l'individuazione di compiti e responsabilità da assegnare ai soggetti individuati in precedenza.

Art. 6 - Obiettivi e finalità del sistema di videosorveglianza

Il sistema di videosorveglianza, in quanto sistema che comporta il trattamento di dati personali, può venire utilizzato (ai sensi dell'art. 6 comma 1 lettera e del Regolamento (UE) n. 2016/679) esclusivamente per il perseguimento delle funzioni istituzionali del titolare del trattamento dei dati.

Le finalità istituzionali che possono essere perseguite mediante l'utilizzo del suddetto impianto sono coerenti e compatibili con le funzioni istituzionali demandate al Titolare dal D.lgs. 18 Agosto 2000, n. 267, dal D.P.R. 24 Luglio 1977, n. 616, dalla Legge 7 Marzo 1986, n. 65 sull'ordinamento della Polizia Locale, dal D.lgs. 30 Aprile 1992, n. 285 e successive modificazioni, nonché dallo Statuto Comunale e dai regolamenti comunali vigenti. In via esemplificativa e non esaustiva le finalità sono:

- attivazione di uno strumento operativo a supporto delle attività di protezione civile sul territorio comunale;

- individuazione, in tempo reale, di luoghi e situazioni di ingorgo e delle cause, per consentire il pronto intervento della Polizia Locale e degli altri soggetti di cui all'art. 12 del D.lgs. n. 285/92;
- comunicazione agli utenti della strada delle vie di maggiore intensità di traffico segnalando eventuali percorsi alternativi e/o ogni altra notizia utile sulla viabilità;
- rilevazione di dati anonimi per l'analisi dei flussi di traffico e per la predisposizione dei piani urbani del traffico;
- vigilanza su aree abusivamente impiegate come discariche di materiali;
- vigilanza (compresa la possibilità di irrogare sanzioni amministrative) sul fenomeno dell'abbandono dei rifiuti;
- videosorveglianza di aree e siti dismessi;
- vigilanza sui luoghi di pubblico transito, in particolare nelle vie, piazze ed aree di mercato, giardini e parchi pubblici, aree antistanti e/o conducenti a scuole di ogni ordine e grado, aree antistanti e/o conducenti a fermate di servizi di linea, ai fini dell'attività ausiliaria di Pubblica Sicurezza e quindi di Polizia di Prevenzione e di Polizia Giudiziaria;
- prevenzione e accertamento di reati;
- prevenzione e rilevazione di atti vandalici;
- tutela del patrimonio comunale, di beni e di persone;
- tutela ambientale;
- rilevazione situazioni di pericolo per la sicurezza urbana, consentendo l'intervento degli operatori;
- raccolta e costituzione di materiale probatorio di natura fotografica e filmica a supporto delle attività di accertamento, contestazione e notificazione di infrazioni, ai sensi degli artt. 13 e 14 della Legge 24 novembre 1981, n. 689;
- sicurezza degli operatori.

Art. 7 – Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità, e finalità.

7.1 Premessa

La verifica del rispetto dei principi di liceità, necessità, non eccedenza e proporzionalità e finalità dovrà venire effettuata periodicamente sia nei confronti del sistema di videosorveglianza nel suo complesso, sia nei confronti di ciascuna telecamera installata.

7.2 Principio di liceità

Affinché sia soddisfatto il principio di liceità, si dovrà periodicamente verificare che:

- le finalità perseguite mediante il sistema di videosorveglianza siano coerenti e compatibili con le funzioni istituzionali di competenza del Titolare;
- la videosorveglianza non avvenga in violazione delle vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata (es. art. 615bis del Codice Penale), di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela;
- la videosorveglianza non abbia luogo in violazione delle tutele riconosciute ai lavoratori, con particolare riferimento a quanto previsto dalla Legge 300/1970 (Statuto dei Lavoratori);
- le riprese o le registrazioni non vengano effettuate in violazione di quanto previsto da disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi;
- la videosorveglianza avvenga nel rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni;
- siano osservati specifici limiti derivanti da disposizioni di legge o di regolamento che prevedono o ipotizzano la possibilità di installare apparecchiature di ripresa locale, aerea o satellitare (d.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, dalla legge 24 aprile 2003, n. 88), disposizioni che, quando sono trattati dati relativi a persone identificate o

identificabili, vanno applicate nel rispetto dei principi affermati dal Codice, in tema per esempio di sicurezza presso stadi e impianti sportivi.

7.3 Principio di necessità

Affinché sia rispettato il principio di necessità deve essere escluso qualsiasi utilizzo superfluo ed evitati eccessi e ridondanze. Inoltre il sistema informatico e ciascuna telecamera deve essere configurata ed utilizzata in maniera tale da non utilizzare dati relativi a soggetti identificabili quando le finalità del trattamento possono essere perseguite raccogliendo solamente dati anonimi; inoltre il software deve essere configurato in modo da cancellare automaticamente e periodicamente i dati eventualmente registrati.

Ulteriori considerazioni da tenere presenti per il rispetto del principio di necessità sono le seguenti:

- l'esigenza di perseguire le finalità deve essere concreta, reale e comprovabile;
- il personale dipendente comunale, non potendo avere una diffusione e una presenza capillare sul territorio, non è in grado di assicurare il monitoraggio e la registrazione continua dei fatti, che solo un sistema di videosorveglianza può assicurare;
- da un punto di vista economico, l'utilizzo di un sistema elettronico di videosorveglianza presenta dei costi sensibilmente inferiori rispetto ai costi derivanti dall'utilizzo di personale dedicato al perseguimento delle finalità indicate in precedenza;
- il sistema di videosorveglianza deve essere configurato per l'utilizzazione al minimo di dati personali e di dati 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.

7.4 Principio di non eccedenza e proporzionalità

Il rispetto dei principi di non eccedenza e proporzionalità si dovrà valutare periodicamente con riferimento ai criteri di seguito elencati:

- il numero e la collocazione delle telecamere devono essere effettivamente commisurate al reale livello di rischio, evitando la rilevazione o la registrazione in aree che non siano soggette a concreti pericoli o che non siano meritevoli di particolare tutela;
- il posizionamento, la tipologia di telecamere, le aree brandeggiabili, l'utilizzo di zoom, quali dati ed eventi rilevare, devono essere rapportati alle concrete finalità ed esigenze, e si dovranno evitare eccedenze; ad esempio si dovrà limitare la possibilità di brandeggio mediante l'impostazione di vincoli o di mascheramenti statici;
- le telecamere devono essere collocate, e più in generale la videosorveglianza deve essere adottata, solo quando altre misure meno "invasive" siano state ponderatamente valutate insufficienti o inattuabili;
- non è consentita l'installazione meramente dimostrativa o artefatta di telecamere non funzionanti o per finzione, che può essere legittimamente oggetto di contestazione;

7.5 Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi, ai sensi dell'art. 5 comma 1 lett. a) del Regolamento Europeo 2016/679; sono pertanto esclusi utilizzi indeterminati, occulti e non legittimi. In particolare il titolare o il responsabile potranno perseguire solo finalità di loro pertinenza.

Potranno essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria). E non finalità generiche o indeterminate, soprattutto quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti.

E' inoltre consentita la videosorveglianza come misura complementare volta a supportare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini o riprese, in caso di atti illeciti.

Art. 8 – Utilizzi esplicitamente vietati

E' fatto in generale divieto di posizionare telecamere, e in ogni caso di utilizzare immagini e registrazioni, in luoghi chiusi, siano essi pubblici o privati. Nel caso si presenti l'esigenza chiaramente dimostrabile e giustificabile, di effettuare riprese in luoghi chiusi pubblici o aperti al pubblico, si dovrà verificare e assicurare che le riprese avvengano nel pieno rispetto dello "Statuto dei lavoratori" e non violino il divieto, da parte del datore di lavoro, di effettuare controlli a distanza sull'attività dei dipendenti.

Art. 8 bis – Deposito di rifiuti

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.

Analogamente, l'utilizzo del sistema di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, l. 24 novembre 1981, n. 689).

Art. 9 – Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada

Gli impianti elettronici di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.

L'utilizzo di tali sistemi è lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate. In conformità alla prassi ed al quadro normativo di settore riguardante talune violazioni del Codice della strada, la normativa vigente in materia di protezione dei dati personali prescrive quanto segue:

- gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;
- le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (es., ai sensi dell'art. 383 del d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (es., pedoni, altri utenti della strada);
- le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;
- le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali

esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;

- le fotografie o le immagini che costituiscono fonte di prova per le violazioni contestate non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;
- in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

Art. 10 - Utilizzo di particolari videocamere mobili

1. Per specifiche finalità connesse alla tutela dell'ordine e della sicurezza urbana, alla prevenzione, all'accertamento e alla repressione dei reati, gli operatori di Polizia Locale possono essere dotati di sistemi di microtelecamere (bodycam) da indossare sulla divisa, per l'eventuale ripresa di situazioni di criticità per la sicurezza propria e altrui.
2. Le videocamere e le schede di memoria di cui sono dotati i sistemi, dovranno essere contraddistinte da un numero seriale che dovrà essere annotato in apposito registro. La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato. Spetta al singolo operatore decidere se attivare la registrazione del dispositivo, in relazione all'evolversi degli scenari di sicurezza che facciano presupporre una criticità.
3. L'operatore deve avvisare i presenti che sta effettuando una registrazione; a tal fine sulla telecamera dovrà essere collocato un adesivo riportante la riproduzione grafica di una telecamera, ovvero dovrà comunicare a voce ai presenti, della registrazione in corso; in quest'ultimo caso tale avviso deve emergere nel contenuto delle immagini registrate.

4. Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare i principi di cui all'art. 5 del Regolamento Europeo sulla privacy e della Direttiva UE 2016/680 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 o distrutti
5. Per specifiche esigenze volte al raggiungimento delle finalità di cui all'articolo 6, La Polizia Locale potrà optare anche per l'utilizzo di dashcam;
6. Le prescrizioni minime generali di utilizzo delle bodycam (telecamere a bordo uomo) e delle dashcam (telecamere a bordo auto) sono descritte nell'Allegato B, che è parte integrante e sostanziale del presente regolamento.

Art. 11 – Accordi con enti pubblici e privati

E' esplicitamente prevista la possibilità da parte del Titolare di stipulare accordi (convenzioni, protocolli di intesa, etc.) con soggetti pubblici e privati, al fine di permettere al Titolare di effettuare la videosorveglianza di aree e territori che non siano di competenza comunale (es. strade provinciali, centri dati in concessione a privati, etc.).

Art. 12 – Tipi di trattamenti autorizzati

Nell'installazione e nell'esercizio del sistema di videosorveglianza, sono autorizzati esclusivamente le seguenti tipologie di trattamenti:

- installazione e attivazione di nuove telecamere;
- creazione e gestione di gruppi e profili di utenti;
- consultazione immagini live da telecamera;
- messa a fuoco e brandeggiamento della telecamera;
- impostazione di limiti al brandeggiamento delle telecamere

- impostazione di zone oscurate staticamente
- registrazione di immagini;
- cancellazione di immagini;
- predisposizione delle soglie temporali e degli eventi di cancellazione immagini;
- consultazione immagini registrate;
- estrazione (duplicazione) immagini registrate;
- definizione aree di motion-detection;
- definizione azioni da eseguire in concomitanza di eventi di motion-detection;
- accensione di sorgenti luminose o ad infrarosso;
- attivazione funzionalità di "speak-ip";
- rilevazione e inventario degli indirizzi ip presenti in rete;
- rilevazione e inventario dei mac address presenti in rete;
- installazione e configurazione di software applicativo;
- installazione e configurazione di software di base;
- installazione di "patch" e "hot fix";
- attivazione collegamenti da remoto;
- interventi generici di manutenzione e configurazione hardware e software
- attivazione e configurazione di meccanismi di tracciatura ("logging");
- estrazione e conservazione di files di log;
- apposizione di forma digitale qualificata e di marcatura temporale e files di log;
- apposizione di forma digitale qualificata e marcatura temporale ad immagini e sequenze filmiche.

Art. 13 – Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati

Le operazioni di trattamento dei dati saranno svolte – a vario titolo – dalle seguenti tipologie di soggetti:

- Titolare del trattamento dei dati personali;
- Designato del trattamento dei dati personali;
- Responsabile del trattamento dei dati personali, sono i soggetti (persone fisiche o giuridiche) terzi al Titolare ai quali sono affidati, alcune operazioni di trattamento dei dati e la messa in atto di alcune misure di sicurezza;
- Autorizzati del trattamento dei dati, sono i soggetti fisici (persone fisiche) che, nominati per iscritto dal Titolare, eseguono una o più operazioni di trattamento dei dati personali;
- Soggetti incaricati della gestione e manutenzione degli strumenti elettronici, denominati anche "Amministratori di sistema";
- Altre Pubbliche Amministrazioni che richiedano di accedere ai dati per lo svolgimento delle loro funzioni istituzionali: in questo caso l'accesso e l'utilizzo dei dati messi a disposizione dal Titolare, avrà luogo sotto la diretta responsabilità e titolarità della Pubblica Amministrazione o del soggetto richiedente: sarà pertanto cura della Pubblica Amministrazione o del soggetto richiedente verificare che l'accesso avvenga esclusivamente per lo svolgimento delle funzioni istituzionali, e non per il perseguimento di interessi o finalità personali o comunque non chiaramente riconducibili allo svolgimento di funzioni istituzionali o di compiti d'ufficio, senza che vi sia abuso d'ufficio. Sarà inoltre cura della Pubblica Amministrazione o del soggetto richiedente, o del soggetto al quale i dati sono comunicati o portati a conoscenza a seguito di motivata richiesta, mettere in atto quanto previsto dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento all'obbligo di designazione degli autorizzati del trattamento, specificando puntualmente per iscritto l'ambito del trattamento consentito e assicurando che le operazioni di trattamento (compresa la mera consultazione, che è comunque una

tipologia di trattamento) e l'accesso ai dati avvenga in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Art. 14 – Accesso ai dati da parte delle forze dell'ordine e dell'Autorità Giudiziaria

La Direttiva 2016/680 del Parlamento europeo e del Consiglio d'Europa, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, introduce la regolamentazione delle protezione delle persone fisiche con riferimento al trattamento dei dati da parte delle autorità a fini di prevenzione, investigazione e repressione di reati.

In base alla direttiva le Forze dell'Ordine o l'Autorità Giudiziaria possono lecitamente richiedere di accedere alle immagini "live", accedere alle immagini registrate ed ottenete copia delle registrazioni, effettuare riprese e registrazioni ad-hoc.

La mancata o tardiva concessione dell'accesso potrà comportare, a carico del soggetto responsabile, il reato di omissione di atti d'ufficio e di ostacolo alle indagini.

Le richieste di accesso/estrazioni dovranno seguire le procedure definite nel presente regolamento.

In ogni caso, l'utilizzo delle immagini da parte di qualsiasi soggetto pubblico che per l'esercizio delle proprie funzioni istituzionali abbia necessità di accedere ai dati, dovrà avvenire conformemente a quanto previsto dal Regolamento Europeo 2016/679 e dal D.Lgs. 196/2003 s.m.i. e più in generale dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento al provvedimento generale del Garante per la protezione dei dati personali del 8 aprile 2010, dedicato alla videosorveglianza.

Art. 15 – Accesso telematico da parte di Carabinieri e Polizia di Stato

E' esplicitamente previsto che i Carabinieri e la Polizia di Stato, previa stipula di una convenzione, possano accedere remotamente in via telematica al sistema di Videosorveglianza, per accelerare i tempi di indagine e per sgravare il personale di Polizia Locale del Titolare; gli accessi dovranno avvenire su base nominativa individuale e dovranno venire tracciati.

Art. 16 – Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento

In generale i soggetti coinvolti nelle operazioni di trattamento dovranno essere nominati per iscritto dal Titolare o dal Responsabile del trattamento dei dati, con atto che specifichi chiaramente compiti e responsabilità assegnate, impartendo loro le adeguate istruzioni. Per quanto riguarda gli autorizzati del trattamento dei dati, oltre ai compiti e alle responsabilità affidate, dovrà essere chiaramente specificato l'ambito del trattamento consentito.

Art. 17 – Designazione degli autorizzati del trattamento dei dati

Coerentemente con quanto prescritto dal punto 3.3.2. del Provvedimento del Garante per le protezioni dei dati personali del 8 aprile 2010, la designazione degli autorizzati dovrà avvenire con modalità che permettano di esplicitare con la massima granularità le tipologie di operazioni alle quali ciascun incaricato risulterà essere abilitato.

Art. 18 – Obblighi degli autorizzati/operatori

L'utilizzo delle telecamere è consentito solo per la sorveglianza di quanto è ubicato oppure si svolge nelle aree pubbliche. Fatti salvi i casi di richiesta degli interessati, i dati registrati possono essere riesaminati, nel limite di tempo ammesso dal presente regolamento, solo in caso di effettiva necessità e per l'esclusivo perseguimento delle finalità di cui all'art. 6. In ogni caso, l'estrazione di immagini potrà avvenire solo in caso di richiesta/autorizzazione scritta, oppure di richiesta proveniente da altra Pubblica Amministrazione, nei casi in cui l'accesso a immagini registrate sia necessario per lo svolgimento delle funzioni istituzionali.

La mancata osservanza degli obblighi di cui al presente articolo potrà comportare l'applicazione di sanzioni disciplinari ed amministrative, e, ove previsto dalla vigente normativa, l'avvio di procedimenti penali.

Art. 19 – Tempi di conservazione delle immagini

In considerazione delle finalità individuate in precedenza, e della necessità di ottemperare al principio di non eccedenza e proporzionalità in tutte le operazioni di trattamento dei dati, le immagini registrate dovranno essere conservate per un tempo massimo di 7 giorni; dovrà comunque essere presente una funzionalità che permetta agevolmente di disattivare la cancellazione automatica – trascorso il tempo massimo di registrazione - delle immagini registrate (ad esempio in concomitanza della registrazione di atti vandalici), senza impedire o menomare la capacità di registrare le immagini "in diretta". E' inoltre prevista la possibilità che i tempi di memorizzazione delle immagini possano venire modificati a seguito di variazioni nelle finalità, di mutate esigenze, oppure di motivata richiesta proveniente da altri soggetti pubblici.

Art. 20 – Cifratura dei dati trasmessi mediante apparati e tecnologie wireless

I dati trasmessi mediante apparati wireless dovranno essere cifrati, in maniera che ne sia garantita la riservatezza.

Art. 21 – Luogo e modalità di memorizzazione delle immagini

La immagini riprese dalle telecamere dovranno venire memorizzate in formato elettronico su un unico (o un numero limitato) supporto di memorizzazione di massa centralizzato e ben individuato all'interno di un unico e ben determinato apparato di tipo "server" (può essere comunque fatta salva la necessità di una memorizzazione "di backup" si un server remoto). Il suddetto server dovrà essere dedicato esclusivamente alla memorizzazione delle immagini registrate dalle telecamere del sistema di videosorveglianza, e non dovrà essere dedicato ad altri scopi. Se non diversamente disposto dal titolare con atto scritto, il server non dovrà essere collegato ad internet, oppure dovrà essere collegato solo in casi e per finalità specifiche e ben individuate, per intervalli di tempo il più possibile contenuti.

Non è consentita la memorizzazione "ordinaria" delle immagini in locale a livello di postazione "client", o comunque su supporti e strumenti diversi dal succitato server centralizzato. La memorizzazione temporanea delle immagini in locale potrà avvenire solo in caso di estrazione di immagini, nel qual caso la copia temporanea locale delle immagini estratte dovrà essere cancellata non appena possibile.

Art. 22 - Criteri e modalità di estrazione delle immagini

L'estrazione di immagini o di intere riprese, mediante duplicazione e senza che vi sia cancellazione delle immagini registrate, è rilasciata a fronte di richiesta scritta e motivata.
La richiesta di estrazione dovrà specificare chiaramente il luogo o la telecamera di registrazione, e un'indicazione dell'intervallo temporale da estrarre e collocare su supporto esterno di memorizzazione di massa, adeguatamente protetto. In generale, le operazioni di estrazione dovranno essere effettuate dall'operatore (appositamente incaricato) in maniera tale che non vi sia accesso o conoscenza, da parte dell'operatore stesso, al contenuto delle immagini da estrarre.
All'atto della consegna al soggetto richiedente del supporto di memorizzazione contenente le immagini estratte, l'operatore o comunque chi materialmente consegnerà il suddetto supporto di memorizzazione, dovrà far firmare e trattenere apposito documento che attesti la consegna e la ricevuta delle immagini estratte; detto documento dovrà fare riferimento alla richiesta originaria di estrazione.
Si dovrà inoltre compilare apposito registro dove si terrà traccia di giorno, data e ora di effettuazione dell'estrazione

Art. 23 – Ottemperanza al Provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativo al controllo dell'operato degli amministratori di sistema.

Per garantire l'ottemperanza a quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 relativo al controllo dell'operato degli amministratori di sistema, il presente Regolamento prevede quanto segue:

- a livello di software di videosorveglianza, deve essere attivato (ed eventualmente configurato) un meccanismo di logging (tracciatura) delle operazioni di amministrazione e gestione di sistema effettuate con profilo di administrator;
- a livello di software di videosorveglianza, il suddetto file di log non deve essere sovrascritto per un periodo minimo di sei mesi;
- il suddetto file di log non dovrà essere per nessun motivo cancellato, modificato o alterato;
- con frequenza al massimo semestrale, si dovrà procedere all'estrazione (copia) del suddetto file di log;
- la copia estratta del file di log dovrà essere generata in un formato non modificabile

Art. 24 – Installazione di nuove telecamere

Preventivamente all''installazione di nuove telecamere si dovrà verificare che:

- i luoghi ripresi;
- le telecamere utilizzate;
- le configurazioni e la possibilità di utilizzo delle telecamere delle riprese e delle registrazioni effettuate;
- soddisfino i principi di liceità, necessità, non eccedenza e proporzionalità e finalità.

Art. 25 – Installazione di telecamere mobili

E' esplicitamente prevista la facoltà, da parte del responsabile del Servizio di Polizia Locale, di installare per brevi periodi e a fronte di determinate esigenze (es. contrasto dello spaccio di stupefacenti, prostituzione, etc.) telecamere mobili, senza ottenere l'autorizzazione preventiva da parte del Sindaco e della Giunta Comunale.
Tali telecamere potranno memorizzare i dati in locale, su apposita scheda SD installata a bordo della telecamera. A seconda delle finalità perseguite, potrà essere possibile non segnalare la presenza di telecamere mediante cartelli informativi.

Art. 26 – Informativa

I cittadini devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa "minima", riportata di seguito. In luoghi diversi dalle aree esterne il modello va integrato con almeno un avviso circostanziato che riporti, oltre agli elementi dell'informativa minima", anche gli altri elementi previsti dall'art. 13 del RE 2016/679.
In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli, in modo tale che gli interessati siano avvertiti della presenza di telecamere prima di transitare nelle aree effettivamente sorvegliate.
Si dovrà assicurare e verificare periodicamente che i cartelli informativi risultino essere agevolmente visibili anche nelle ore notturne o crepuscolari, o perché illuminati di sorgenti luminose (illuminazione pubblica, faretti, etc.) e/o perché realizzati su supporto catarifrangente.

Art. 27 - Riscontro all'interessato

In relazione al trattamento dei dati personali l'interessato ha diritto come previsto dall'articolo 15 del Regolamento Europeo sulla privacy:

a. di conoscere l'esistenza di trattamenti che possono riguardarlo;
b. di ottenere, a cura del Titolare senza alcun ritardo e comunque non oltre 30 (trenta) giorni dalla data di ricezione della richiesta:
c. I. la conferma dell'esistenza o meno di dati personali che lo riguardano e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e della finalità su cui si basa il trattamento;
d. II. la cancellazione, 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;
e. c. di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano ancorché pertinenti allo scopo della raccolta.

La richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con un intervallo di tempo non minore di 90 (novanta) giorni.
Le istanze degli interessati, di cui al presente articolo, devono essere presentate all'ufficio protocollo in carta semplice, anche mediante lettera raccomandata, fax, pec, o negli altri modi previsti dalla legge, e devono essere indirizzate al Titolare del trattamento.
I diritti riferiti ai dati personali concernenti persone decedute, possono essere esercitati da chiunque sia legittimato.
Nell'esercizio dei diritti di cui al presente articolo, l'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni. L'interessato può, altresì, farsi assistere da persona di fiducia.
Per ciascuna delle richieste può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, definiti con atto formale della Giunta comunale secondo le modalità previste dalla normativa vigente.
Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante, secondo quanto disposto dal Codice Privacy, e fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Art. 28 – Requisiti minimi sul luogo di collocazione del server

Il server di memorizzazione delle immagini dovrà essere fisicamente collocato all'interno di un locale che fornisca adeguate garanzie di sicurezza fisica e perimetrale. Di seguito si riportano i requisiti minimi che il locale dovrà soddisfare:

- locale di norma chiuso a chiave, con serratura e chiave funzionante;
- assenza di carta, cartoni o altro materiale facilmente infiammabile all'interno del locale;
- presenza nelle vicinanze di almeno un estintore non a polvere, funzionante e regolarmente revisionato con frequenza almeno semestrale;

In aggiunta a quanto elencato, è auspicabile (ancorché non strettamente obbligatoria) la presenza di quanto segue:

- allarme volumetrico (attivato dalla variazione della volumetria all'interno dei locali) o di prossimità;
- collegamento dei sensori e dell'allarme con centrale operativa di sicurezza oppure con le forze dell'ordine.

Art. 29 – Requisiti minimi sugli strumenti elettronici, informatici e telematici

Gli strumenti elettronici, informatici e telematici utilizzati nelle operazioni di trattamento dei dati, dovranno soddisfare i seguenti requisiti minimi:

- sistema operativo server e client non obsoleto e con supporto attivo da parte del fornitore; non sono consentiti sistemi operativi obsoleti o poco sicuri e non aggiornati;
- presenza di almeno due profili distinti: uno di tipo "administrator" e uno di tipo "utente normale", sia a livello di sistema operativo sia a livello di programma applicativo;
- assegnazione e utilizzo delle user-id su base strettamente personale e non di gruppo;
- possibilità di individuare e rimuovere periodicamente le vulnerabilità e le configurazioni poco sicure a livello applicativo e di sistema operativo;
- protezione adeguata da virus e codici maligni;
- protezione perimetrale adeguata in caso di apertura, anche temporanea, ad Internet.

Art. 30 – Cessazione del trattamento

In caso di cessazione del trattamento, i dati dovranno essere distrutti, ad eccezione di quelli per i quali siano in corso o vi siano state in passato richieste di estrazione, che dovranno essere conservati a cura del titolare per fini di documentazione e riscontro.

Art. 31 – Limiti alla utilizzabilità dei dati personali

I limiti all'utilizzabilità dei dati personali sono quelli recati dal Regolamento Europeo sulla Privacy UE 2016/679

Art. 32 – Danni cagionati per effetto del trattamento dei dati personali

La materia è disciplinata dall'art.79 del Regolamento Europeo sulla privacy.
In particolare, chiunque subisca un danno materiale o immateriale per effetto del trattamento dei 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 RGDP.
Il titolare o il responsabile del trattamento è esonerato dalle 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'art. 79, paragrafo 2 del RGDP.

Art. 33 – Comunicazione

La comunicazione di dati personali da parte del titolare ad altri soggetti pubblici è ammessa quando è prevista da norma di legge o di regolamento attuativo di norma di legge, oppure quando risulti comunque necessaria per lo svolgimento delle funzioni istituzionali.
In mancanza di una tale norma, la comunicazione è ammessa quando è necessaria ed esclusivamente per lo svolgimento delle funzioni istituzionali nei modi e nei tempi previsti dal Codice Privacy.
Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone autorizzate per iscritto a compiere le operazioni del trattamento dal Titolare o dal Responsabile e che operano sotto la loro diretta autorità.
E' in ogni caso fatta salva la comunicazione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'Art. 58, comma 2, del Codice Privacy, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Art. 34 – Tutela amministrativa e giurisdizionale

Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dal Regolamento europeo sulla privacy UE 2016/679 e al Codice in materia di protezione dei dati personali D.Lgs. 30 giugno 2003, n. 196 s.m.i..

Art. 35 – Modifiche e integrazioni regolamentari

Il presente regolamento dovrà essere adeguato per recepire eventuali modifiche alla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento alle disposizioni e ai provvedimenti emanati dal Garante per la protezione dei dati personali.
Inoltre, il presente regolamento dovrà venire modificato nel caso dovessero mutare le finalità del sistema di videosorveglianza.

Art. 36 – Norme finali

Per quanto non disciplinato dal presente regolamento, si rinvia al Regolamento europeo sulla privacy UE 2016/679 e al Codice in materia di protezione dei dati personali D.Lgs. 30 giugno 2003, n. 196 s.m.i., e al provvedimento generale sulla videosorveglianza emesso dal Garante per la protezione dei dati personali in data 8 aprile 2010.

Art. 37 – Pubblicità e conoscibilità del regolamento

Il regime di eventuale pubblicità e conoscibilità del presente regolamento è disciplinato dallo Statuto del Comune di Robbiate, Paderno d'Adda, Verderio e dalla disciplina rilevante in materia di accesso agli atti e documenti amministrativi.