Comune di Albiate

Provincia di Monza e della Brianza

REGOLAMENTO COMUNALE
PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA URBANA INTEGRATA SUL TERRITORIO COMUNALE

Approvato dal Consiglio Comunale con deliberazione n. ..... in data ...../...../.....

Sommario

CAPO I PRINCIPI GENERALI 4
Art. 1 – Oggetto 4
Art. 2 – Definizioni 5
Art. 3 – Finalità e sistemi di sorveglianza 6
Art. 4 - Ambito di validità e di applicazione del presente regolamento 7
Art. 5 – Trattamento dei dati personali 7
Art. 6 – Designato e Autorizzato 9
Art. 7 – Funzioni del designato 9
Art. 8 – Persone autorizzate ad accedere alla sala di controllo 11
Art. 9 – Soggetti autorizzati al trattamento e dei preposti alla gestione dell'impianto di videosorveglianza 11
CAPO III TRATTAMENTO DEI DATI PERSONALI 13
Art. 10 – Diretta visione delle immagini 13
Art. 11 – Modalità di raccolta e requisiti dei dati personali 13
Art. 12– Modalità da adottare per i dati video ripresi 14
Art. 13 – Comunicazione 15
Art. 14 – Limiti alla utilizzabilità di dati personali 15
Art. 15 – Tipi di trattamenti autorizzati 15
CAPO IV DIRITTI DEGLI INTERESSATI 17
Art. 16-Informativa 17
Art. 17 – Informazioni rese al momento della raccolta 17
Art. 18 – Diritti dell'interessato 17
CAPO V MISURE DI SICUREZZA 18
Art. 19 – Cifratura dei dati trasmessi mediante apparati e tecnologie wireless 18
Art. 20– Luogo e modalità di memorizzazione delle immagini 18
Art. 21 Criteri e modalità di estrazione delle immagini 19
Art. 22– Ottemperanza al Provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativo al controllo dell'operato degli amministratori di sistema. 19
Art. 23 – Requisiti minimi sul luogo di collocazione del server 20
Art. 24 – Requisiti minimi sugli strumenti elettronici, informatici e telematici. 20
Art. 25 – Obblighi degli autorizzati 21
Art. 26 – Sicurezza dei dati 21
Art. 27 – Cessazione del trattamento dei dati 21
Art. 28 – Trasmissione dei video 22

Art. 29 – Accordi con enti pubblici e privati 23
Art. 30 – Accesso ai dati da parte delle forze dell'ordine e dell'Autorità Giudiziaria 23
Art. 31 – Accesso telematico da parte delle Autorità Giudiziarie 23
CAPO VII DISPOSITIVI DI VIDEOSORVEGLIANZA 24
Art. 32 – Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada. 24
Art. 33– Utilizzi particolari 25
Art. 34 Abbandono e conferimento dei rifiuti. 25
Art. 35 Utilizzo di particolari videocamere mobili Body Cam e Dash Cam, e Droni. 25
Art. 36 Foto trappole 26
CAPO VIII GESTIONE DEL DATA BREACH 27
Art. 37 – Perdita dei dati – Data Breach 27
Art. 38 – Gestione della comunicazione del data breach 27
Art.39- Identificazione e indagine preliminare 27
Art 40 - Contenimento, Recovery e risk assessment 28
Art. 41 - Eventuale notifica all'Autorità Garante competente 28
Art. 42 Eventuale comunicazione agli interessati 29
Art. 43 - Documentazione della violazione 29
CAPO IX TUTELA AMMINISTRATIVA E GIURISDIZIONALE - MODIFICHE 30
Art. 44 – Tutela 30
Art. 45– Modifiche regolamentari 30
Art. 46 – Danni cagionati per effetto del trattamento di dati personali 30
CAPO X DISPOSIZIONI FINALI 31
Art. 47 – Partenariato pubblico privato per il potenziamento della videosorveglianza ad uso pubblico 31
Art. 48 – Tutela dei dati personali 31
Art. 49 – Rinvio dinamico 31
Art. 50– Entrata in vigore 31

CAPO I

PRINCIPI GENERALI

Art. 1 – Oggetto

1. Il presente regolamento disciplina il trattamento dei dati personali, realizzato mediante l'impianto di videosorveglianza, attivato nel territorio urbano del Comune di Albiate

2. Per tutto quanto non è dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dal:

- Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "*Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia*";
- Regolamento UE n. 2016/679 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;
- 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;
- D.Lgs. 30 giugno 2003, n, 196, come modificato dal D.Lgs. n. 101 del 10 agosto 2018, recante: "Codice in materia di protezione dei dati personali e successive modificazioni;
- D.Lgs. 18/05/2018, n. 51 recante: "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."
- art. 54 del D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni;
- decalogo del 29 novembre 2000 promosso dal Garante per la protezione di dati personali;
- circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/A/471;
- D.L. 23 febbraio 2009, n. 11, recante: "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori ", ed in particolare dall'art. 6;

- D.L. 20 febbraio 2017 n 14 recante “Disposizioni urgenti in materia di sicurezza delle città”
- “Provvedimento in materia di videosorveglianza” emanato dal garante per la protezione dei dati personali in data 8 aprile 2010.

Art. 2 – Definizioni

1. Ai fini del presente regolamento si intende:

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

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

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

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

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

f) per «responsabile del trattamento», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

g) per «incaricato del trattamento», la persona fisica che abbia accesso a dati personali;

h) per “interessato”, la persona fisica identificata o identificabile cui si riferiscono i dati personali oggetto di trattamento;

i) per «terzo», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

j) per «violazione dei dati personali», la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

k) per «comunicazione», il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

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

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

Art. 3 – Finalità e sistemi di sorveglianza

1. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l’attivazione di un impianto di videosorveglianza nel territorio urbano, gestito dal Comune di Albiate-Servizio di Polizia Locale che in prospettiva potrà essere collegato alla centrale operativa delle Forze dell’Ordine, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all’identità personale. Il trattamento dei dati è effettuato per motivi di interesse pubblico rilevanti, finalizzati alla sicurezza della popolazione e alla salvaguardia della vita e dell'incolumità fisica ai sensi dell'art. 2 sexies del D.Lgs. n. 196/03; nonché per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali ai sensi dell’art. 1 comma 2 del n. D.lgs 51/2018. Garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento. Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l’utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l’interessato solo in caso di necessità.

2. L’utilizzo degli impianti di videosorveglianza è finalizzato a:

a) prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 e delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del d.lvo 267/2000;

b) prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado e abbandono di rifiuti, e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nei regolamenti locali in genere e nelle ordinanze sindacali;

c) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;

d) tutelare l'ordine, il decoro e la quiete pubblica;

e) controllare aree specifiche del territorio comunale;

f) monitorare i flussi di traffico e monitorare l'accesso alle zone a traffico limitato;

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

h) attivare uno strumento operativo di protezione civile sul territorio comunale.

3. Nei locali delle forze dell'ordine sarà posizionato un monitor per la visione in diretta delle immagini riprese dalle telecamere.

4. Possono essere installati sistemi integrati, sistemi intelligenti e sistemi per rilevare delle violazioni al codice della strada.

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 del Comune di Albiate e all'interno del territorio dell'ente stesso.

Art. 5 – Trattamento dei dati personali

1. Il trattamento dei dati personali è effettuato a seguito dell'attivazione di un impianto di videosorveglianza.

2. Le finalità istituzionali del suddetto impianto sono del tutto conformi alle funzioni istituzionali demandate al Comune di Albiate, in particolare dal D.Lgs. 18 agosto 2000 n. 267, dal D.P.R. 24 luglio 1977 n. 616, dal D.Lgs. 31 marzo 1998 n. 112, dalla legge 7 marzo 1986 n. 65 sull'ordinamento della Polizia Municipale, dalla normativa regionale, nonché dallo statuto e dai regolamenti comunali. La disponibilità tempestiva di immagini presso il Servizio della Polizia Locale e i locali delle forze armate costituisce inoltre uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale e delle altre Forze dell'Ordine.

3. La videosorveglianza effettua una vera e propria attività di vigilanza su persone e beni, sostituendo, in tutto o in parte, la presenza umana sul posto.

4. La risoluzione della ripresa sarà bassa nel caso che le telecamere siano state installate per verificare traffico, ingorghi, esondazioni, ecc. La risoluzione sarà alta per telecamere posizionate al fine della sicurezza urbana.

5. Nelle scuole gli impianti possono essere attivati esclusivamente negli orari di chiusura degli edifici, fatte salve necessità di giustizia.

6. Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese televisive e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.

7. Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970 e successive modificazioni) per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

CAPO II
SOGGETTI DEL TRATTAMENTO

Art. 6 – Designato e Autorizzato

1. L'Agente di Polizia Locale, nominato del Sindaco, domiciliato in ragione delle funzioni svolte in Albiate, presso l'Ufficio di Polizia Locale, è individuato quale Designato del trattamento dei dati personali rilevati, ai sensi per gli effetti dell'art. 2, comma 1, lett. e).

2. Il designato deve rispettare pienamente quanto previsto, in tema di trattamento dei dati personali, dalle leggi vigenti, ivi incluso il profilo della sicurezza e dalle disposizioni del presente regolamento.

3. Il designato procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

4. I compiti affidati al designato devono essere analiticamente specificati per iscritto, in sede di designazione.

5. Gli autorizzati al materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del titolare o del designato.

6. Il designato custodisce le chiavi per l'accesso ai locali della centrale di controllo, le chiavi degli armadi per la conservazione delle immagini, nonché le parole chiave per l'utilizzo dei sistemi.

Art. 7 – Funzioni del designato

1. La nomina è effettuata con atto del Sindaco, nel quale sono analiticamente specificati i compiti affidati al designato. In particolare, il designato del trattamento:

- individuerà e nominerà con propri atti i soggetti autorizzati al trattamento, impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, RGPD, nonché all'art 18 del D.lgs 51/2018; detti soggetti saranno opportunamente istruiti e formati da parte del designato 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;

- provvede a rendere l'informativa "minima" agli interessati secondo quanto definito al precedente art. 6;

- verifica e controlla che il trattamento dei dati effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui all'art. 5 del RGPD nonché all'art 3 del D.lgs 51/2018 e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente;

garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;

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

- tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD; nonché dell'art. 25 del D.Lgs 51/2018

- assiste il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;

- assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;

- garantisce l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;

- assicura l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;

- assiste il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;

- assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e del precedente art. 6 del presente Regolamento e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;

- 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;

- 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;

- mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;

- è responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

- assicura 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;

- garantisce la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale autorizzato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;

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

Art. 8 – Persone autorizzate ad accedere alla sala di controllo

1. L'accesso alla sala di controllo è consentito solamente al personale in servizio della Polizia Locale

2. Eventuali accessi di persone diverse da quelli innanzi indicate devono essere autorizzati, per iscritto, dal designato.

3. Possono essere autorizzati all'accesso solo incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui al presente regolamento, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali e il personale delle forze dell'ordine.

4. Il Responsabile del Servizio di Polizia Locale designato è responsabile della gestione e del trattamento, impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.

5. Il designato e gli autorizzati di cui al presente regolamento vigilano sul puntuale rispetto delle istruzioni e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 9 – Soggetti autorizzati al trattamento e dei preposti alla gestione dell'impianto di videosorveglianza

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

2. In particolare, i soggetti autorizzati devono:

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

- conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;

- custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;

- evitare di creare banche dati nuove senza autorizzazione espressa del designato del trattamento dei dati;

- mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;

- conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;

- fornire al Titolare dei dati trattati ed al Responsabile della Protezione dei dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

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

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

5. eventuali soggetti che svolgono, fra il personale dell'ente, mansioni di amministratore di sistema verranno appositamente designati dal titolare del trattamento;

6. Nell'ambito dei designati/autorizzati, verranno individuati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle password e delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti contenenti le immagini.

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Art. 10 – Diretta visione delle immagini

1. La diretta visualizzazione delle immagini rilevate con i sistemi di videosorveglianza nelle sale o centrali operative è limitata ad obiettivi particolarmente sensibili e strategici per la sicurezza urbana o in presenza del requisito di pubblico interesse (necessità, pertinenza, non eccedenza dei dati o dei trattamenti).

2. Il designato o gli l'autorizzati si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto.

3. Il flusso dei dati può giungere agli organi di Polizia locale, in grado di garantire i servizi di monitoraggio ed il conseguente, eventuale, allertamento della sala.

Art. 11 – Modalità di raccolta e requisiti dei dati personali

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

2.L'utilizzo del brandeggio da parte dei soggetti autorizzati avviene nel rispetto dei limiti previsti dal presente regolamento.

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

4. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa sono inviati presso la sede del Corpo di Polizia Locale o datacenter individuato appositamente dove sono registrati su appositi server. I video possono essere visionati dalle Forze dell'ordine a ciò autorizzate. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, ai fini del soddisfacimento delle finalità di cui all'articolo 3 del presente regolamento.

6. I dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;

- raccolti e registrati per le finalità di cui all'art. 3 del presente Regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;

- raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

7. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata al massimo 7 giorni, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

8. Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza pubblica, alla luce delle richiamate disposizioni normative, il termine massimo di durata della conservazione e definito a seconda dello scenario concreto, fatte salve specifiche esigenze di ulteriore conservazione.

9. In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Responsabile potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai sette giorni.

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

11. In caso di cessazione del trattamento, i dati personali sono distrutti.

Art. 12– Modalità da adottare per i dati video ripresi

1. I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.

2. L'accesso alle immagini da parte del designato e degli autorizzati del trattamento dei dati si limita alle attività oggetto della sorveglianza; eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione.

3. Nel caso le immagini siano conservate, i relativi supporti che dovranno essere crittografati, vengono custoditi per l'intera durata della conservazione, in un armadio o simile struttura dotato di serratura, apribile solo dal designato e dagli autorizzati del trattamento dei dati.

4. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate; le operazioni di cancellazione devono essere effettuate esclusivamente all'interno dell'ambiente a ciò deputato sito all'interno del Servizio di Polizia Locale.

5. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile, non permettendo il recupero dei dati in esso presenti.

6. L'accesso alle immagini ed ai dati personali è consentito:

- al Designato ed agli autorizzati dello specifico trattamento;
- ai preposti alle indagini dell'Autorità Giudiziaria e di Polizia;
- al responsabile esterno incaricato della manutenzione dell'impianto nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione;

7. Tutti gli accessi alla visione saranno documentati e registrati tramite sistema automatico di log.

9. Non possono essere rilasciate copie delle immagini registrate concernenti altri soggetti diversi dall'interessato, salvi i casi particolarmente meritevoli di tutela.

Art. 13 – Comunicazione

1. La comunicazione dei dati personali da parte dell'Ente a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria ed esclusivamente per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 2 ter del D.Lgs. n. 196/03.

3. È in ogni caso fatta salva la comunicazione o diffusione di dati richieste, 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 D.Lgs. 30/6/2003, n. 196 per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Art. 14 – Limiti alla utilizzabilità di dati personali

1. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati ai sensi dell'art. 2 decies del D.Dgs. n. 196/03, salvo quanto previsto dall'art. 160 bis dello stesso decreto.

Art. 15 – 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.

CAPO IV

DIRITTI DEGLI INTERESSATI

Art. 16-Informativa

1. I soggetti interessati, che stanno per accedere o che si trovano in una zona videosorvegliata, devono essere informati mediante appositi cartelli conformi ai modelli approvati dall'Autorità garante per la protezione dei dati personali.

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

3. Sul sito istituzionale del Comune è pubblicata l'informativa completa contenente le modalità e le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e al D.Lgs. n. 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. Inoltre, viene riportata l'indicazione della esatta collocazione di tutti gli impianti di videosorveglianza comunale con indicazione della natura e finalità di essi.

Art. 17 – Informazioni rese al momento della raccolta

1. L'Ente in ottemperanza a quanto disposto dall'art. 13 del Reg. UE n. 679/16 (G.D.P.R.) e del D.Lgs. n. 51/2018, si obbliga ad affiggere un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.

2. In presenza di più telecamere in relazione alla vastità dell'area oggetto di rilevazione, sono installati più cartelli.

Art. 18 – Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:

a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;

b) di essere informato sugli estremi identificativi del titolare e del designato al trattamento, oltre che sulle finalità e le modalità del trattamento dei dati;

c) di ottenere:

- la conferma dell'esistenza o meno di dati personali che lo riguardano;

- la trasmissione in forma intelligibile dei medesimi dati e della loro origine;

- l'informazione sulle procedure adottate in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento, 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;

2. In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

3. Per ciascuna delle richieste di cui al comma 1, lett. c), 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, secondo le modalità previste dalla normativa vigente.

4. 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.

5. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.

6. Le istanze di cui al presente articolo possono essere trasmesse al titolare o al designato anche mediante lettera raccomandata, o posta elettronica o comunicata oralmente.

CAPO V
MISURE DI SICUREZZA

Art. 19 – 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. 20– 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" anche su 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 è consentita solamente in aree appositamente dedicate del server, nel qual caso la copia temporanea delle immagini estratte dovrà essere cancellata non appena possibile.

Art. 21 Criteri e modalità di estrazione delle immagini

L'estrazione di immagini o di intere riprese, mediante duplicazione, potrà avvenire solo in presenza di autorizzazione scritta da parte del Titolare del trattamento o del designato, rilasciata a fronte di richiesta scritta e motivata.

Alle registrazioni delle immagini video, il sistema appone l'impronta digitale su ciascun frame; tale impronta è ottenuta utilizzando l'algoritmo di HASH MD5 in base al contenuto del frame. Tutto ciò a garanzia dell'originalità della copia.

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.

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. 22– 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 2 anni;
- il suddetto file di log non dovrà essere per nessun motivo cancellato, modificato o alterato durante il suddetto periodo;

la copia estratta del file di log dovrà essere generata in un formato non modificabile.

Art. 23 – 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. 24 – 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. 25 – Obblighi degli autorizzati

1. L'utilizzo del brandeggio da parte degli operatori e degli incaricati al trattamento dovrà essere conforme ai limiti indicati nel presente regolamento e dalle norme in materia.

2. L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolge nei luoghi pubblici o aperti al pubblico, mentre esso non è ammesso nelle proprietà private.

3. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui agli artt. 3 e 5 e a seguito di regolare autorizzazione di volta in volta dal designato.

4. La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

Art. 26 – Sicurezza dei dati

1. I dati personali oggetto di trattamento sono custoditi ai sensi e per gli effetti del precedente art. 11. Alla sala controllo del Servizio della Polizia Locale, dove sono custoditi i dati e le immagini registrate, può accedere solo ed esclusivamente il personale in servizio della Polizia Locale, debitamente istruito sull'utilizzo dell'impianto e debitamente incaricato ed autorizzato per iscritto dal Titolare del trattamento o designato.

2. Il designato alla gestione e al trattamento impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.

3. Il designato al trattamento designa e nomina gli autorizzati in numero sufficiente a garantire la gestione del servizio di videosorveglianza e dei sistemi di lettura targhe nell'ambito degli operatori di Polizia locale.

4. Gli autorizzati andranno nominati tra gli agenti in servizio, che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati. La gestione degli impianti di videosorveglianza e dei sistemi di lettura targhe è riservata agli organi di Polizia Locale, aventi qualifica di Agenti di polizia giudiziaria ai sensi dell'art. 55 del c.p.p.

Art. 27 – Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:

a) distrutti;

b) conservati per fini esclusivamente istituzionali dell'impianto attivato, secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e dall'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.

Art. 28 – Trasmissione dei video

Al fine di garantire la sicurezza della trasmissione dei dati, gli stessi dovranno essere comunicati adottando le opportune misure di sicurezza volta alla tutela del dato

CAPO VI
ACCESSO AI DATI DA PARTE DI ALTRI SOGGETTI

Art. 29 – Accordi con enti pubblici e privati

È 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. 30 – 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".
- Le richieste di accesso/estrazioni dovranno seguire le procedure definite nel presente regolamento in particolare all'art 21, ed essere autorizzate dal Titolare o dal designato.
- 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. 31 – Accesso telematico da parte delle Autorità Giudiziarie

È esplicitamente previsto che le Autorità Giudiziarie, previa stipula di una convenzione / accordo interforze stipulata tra le parti possano accedere remotamente in via telematica al sistema di Videosorveglianza, per accelerare i tempi di indagine e per sgravare il personale di Polizia Locale, gli accessi dovranno avvenire su base nominativa individuale, e dovranno venire tracciati (log).

CAPO VII
DISPOSITIVI DI VIDEOSORVEGLIANZA

Art. 32 – 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. 33– Utilizzi particolari

Qualora il sistema di videosorveglianza venga utilizzato a fini di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, si dovrà rispettare quanto dettato dal d.P.R. 22 giugno 1999, n. 250. Tale normativa impone al titolare del trattamento dei dati di rilasciare una specifica autorizzazione amministrativa nonché di limitare la raccolta dei dati sugli accessi rilevando le immagini solo in caso di infrazione (art. 3 d.P.R. n. 250/1999). In questo specifico caso e utilizzo, i dati trattati potranno essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso e si potrà accedere ad essi solo a fini di polizia giudiziaria o di indagine penale.

Art. 34 Abbandono e conferimento dei rifiuti.

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

2.Analogamente, l'utilizzo di sistemi di videosorveglianza sarà lecito laddove 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, legge 24 novembre 1981, n. 689).

Art. 35 Utilizzo di particolari videocamere mobili Body Cam e Dash Cam, e Droni.

1.Per specifiche finalità concernenti la tutela dell'ordine e della sicurezza urbana e pubblica, la prevenzione, l'accertamento e la repressione dei reati, gli operatori di Polizia Locale possono essere dotati di sistemi di microtelecamere da indossare sulla divisa, per l’eventuale ripresa di situazioni di criticità per la sicurezza propria e altrui.

2.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.

3. Gli operatori di Polizia Locale possono utilizzare, per i servizi a maggior rischio operativo, delle Body Cam e delle Dash Cam in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016, prot. n. 49612, ed al parere preventivo pubblicato il 31/7/2014 (docweb 3423775) con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati (essendo stato abrogato l'articolo 53 del Codice) è ricondotto nell'ambito del D.lgs 51/2018 trattandosi di "dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela all'ordine e della sicurezza pubblica, nonché di polizia giudiziaria"

4. Gli operatori di Polizia Locale possono utilizzare le riprese tramite droni, per visualizzare aree non facilmente accessibili, o per avere una visione alternativa (aerea) dello scenario operativo (p.e. di un incidente). Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D.lgs 51/2018 che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.

Art. 36 Foto trappole

Gli apparati "Telecamere modulari" (foto trappole) vengono posizionati secondo necessità, esclusivamente nei luoghi teatro di illeciti penali o amministrativi, quando questi ultimi non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D.lgs 51/2018 che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree

CAPO VIII

GESTIONE DEL DATA BREACH

Art. 37 – Perdita dei dati – Data Breach

Il personale che provvede al concreto utilizzo dei dispositivi di videosorveglia, dovrà segnalare immediatamente al Designato dell'Ente, qualsiasi anomalia, malfunzionamento, nonché la perdita – anche parziale – accidentale o volontaria di dati (Data Breach).

Art. 38 – Gestione della comunicazione del data breach

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Nel caso in cui una delle figure abilitate al trattamento si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico, congiuntamente ne daranno comunicazione al titolare del trattamento mediante la compilazione di apposito modulo. Lo stesso modulo verrà inviato a mezzo mail o pec all'indirizzo del DPO.

Art.39- Identificazione e indagine preliminare

Il modulo di cui all'art. 37, debitamente compilato, permetterà al Titolare del trattamento insieme al DPO, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento dell'Autorità garante per la Protezione dei dati.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento insieme al DPO dovrà coinvolgere anche il Responsabile dell'Ufficio IT o un suo delegato in caso di assenza.

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nel modulo, quali:

- la data di scoperta della violazione (tempestività);
- Il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;

- la descrizione di eventuali azioni già poste in essere.

Art 40 - Contenimento, Recovery e risk assessment

Il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il DPO valuteranno la gravità della violazione utilizzando il Modulo di valutazione del Rischio connesso al Data Breach (disponibili sul sito dell'Autorità garante della protezione dei dati) che dovrà essere esaminato, unitamente al modulo di cui art. 37 tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 del GDPR .

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Art. 41 - Eventuale notifica all'Autorità Garante competente

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita, secondo quanto prescritto dal Regolamento (UE) 2016/679, (Denominazione dell'ente) dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

Pertanto, il Titolare del trattamento e il DPO invieranno la corretta modulistica all'Autorità Garante per la protezione dei dati personali così da effettuare la notificazione del data breach.

Art. 42 Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'Ente dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento e il DPO dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento e il DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e- mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Art. 43 - Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente, l'Ente sarà tenuto a documentarlo.

Tale documentazione sarà affidata al Titolare del trattamento o da un suo delegato con l'ausilio del Responsabile dell'Ufficio IT (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta del Registro dei Data Breach, secondo le informazioni ivi riportate: (i) n. violazione; (ii) data violazione; (iii) natura della violazione; (iv) categoria di interessati; (v) categoria di dati personali coinvolti; (vi) numero approssimativo di registrazioni dei dati personali; (vii) conseguenze della violazione; (viii) contromisure adottate; (ix) se sia stata effettuata notifica all'Autorità Garante Privacy; (x) se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

CAPO IX

TUTELA AMMINISTRATIVA E GIURISDIZIONALE - MODIFICHE

Art. 44 – Tutela

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

2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati personali.

Art. 45– Modifiche regolamentari

1. I contenuti del presente regolamento sono aggiornati nei casi di aggiornamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali del Consiglio Comunale dovranno essere immediatamente recepiti.

Art. 46 – Danni cagionati per effetto del trattamento di dati personali

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

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

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

CAPO X
DISPOSIZIONI FINALI

Art. 47 – Partenariato pubblico privato per il potenziamento della videosorveglianza ad uso pubblico

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

Art. 48 – Tutela dei dati personali

1. Il comune garantisce, nelle forme ritenute più idonee, che il trattamento dei dati personali in suo possesso si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, ai sensi delle vigenti disposizioni in materia.

Art. 49 – Rinvio dinamico

1. Le disposizioni del presente regolamento si intendono modificate per effetto di sopravvenute norme vincolanti statali e regionali.

2. In tali casi, in attesa della formale modificazione del presente regolamento, si applica la normativa sopra ordinata.

Art. 50– Entrata in vigore

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

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