Comune di Buttigliera Alta

REGOLAMENTO PER L'UTILIZZO DEGLI IMPIANTI DI VIDEOSORVEGLIANZA CITTADINA

Delibera del Consiglio Comunale n. 32 del 30/06/2021

Indice

Articolo 1 - Premessa

1) Il presente regolamento disciplina le modalità di raccolta, trattamento e conservazione dei dati personali mediante sistemi di videosorveglianza gestiti, nell'ambito del proprio territorio, dal Comando di Polizia Locale del Comune di Buttigliera Alta.

2) Il trattamento dei dati personali è effettuato a seguito dell'attivazione di sistemi di videosorveglianza che fanno uso di telecamere fisse e/o mobili ovvero di ulteriori sistemi di registrazione delle immagini meglio specificati *infra*.

3) Un sistema di videosorveglianza è costituito da dispositivi analogici e digitali nonché da software per l'acquisizione e registrazione di immagini.

4) I suoi componenti sono categorizzabili come segue:

   a. Ambiente video per l'acquisizione delle immagini, le interconnessioni e la gestione immagini:

      - s'intende acquisizione delle immagini il complesso di operazioni atte ad imprimere una o una sequenza di immagini acquisite mediante strumenti di cattura in un formato logico fruibile dal sistema;
      - le interconnessioni comprendono il complesso di trasmissioni di dati all'interno dell'ambiente video, ovvero connessioni e comunicazioni (esempi di connessioni sono cavi, reti digitali e trasmissioni wireless. Le comunicazioni descrivono tutti i segnali video e dati di controllo, che potrebbero essere digitali o analogici);
      - la gestione delle immagini comprende l'analisi, la conservazione e l'estrapolazione di un'immagine o di una sequenza di immagini.

   b. Dal punto di vista della gestione del sistema, un sistema di videosorveglianza ha le seguenti funzioni logiche:

      - gestione dei dati e delle attività, compresa la gestione dei comandi degli operatori e delle attività generate dal sistema (procedure di allarme, operatori di allarme);
      - le interfacce con altri sistemi che potrebbero includere la connessione ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) o non legati alla sicurezza (sistemi di gestione edifici, riconoscimento automatico delle targhe).

   c. La sicurezza di un sistema di videosorveglianza consiste nella riservatezza, nell'integrità e nella disponibilità del sistema e dei dati:

      - la sicurezza del sistema comprende la sicurezza fisica di tutti i componenti del sistema e il controllo dell'accesso al sistema di videosorveglianza, o la sicurezza dei dati comprende la prevenzione della perdita o della manipolazione dei dati.

5) Per il presente regolamento, con sistema di videosorveglianza s'intende il complesso di sistemi finalizzati alla vigilanza in remoto mediante dispositivi di ripresa, captazione ed eventuale conseguente analisi di immagini collegati ad un centro di controllo e coordinamento gestito dal Comando di Polizia Locale di Buttigliera Alta.

6) Il presente regolamento è diretto, tra le altre cose, a garantire che il trattamento dei dati personali, effettuato mediante i sistemi di videosorveglianza installati, manutenuti e gestiti dal Comune di Buttigliera Alta si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità

personale, mediante l'adozione di misure tecniche ed organizzative idonee ai sensi dell'art. 32 del RGPD.

7) Il trattamento dei dati personali nell'ambito definito dal presente regolamento non necessita del consenso degli interessati in quanto viene effettuato in forza delle seguenti basi giuridiche:
    - L'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri ai sensi dell'art. 6 par. 2 lett. e);
    - l'adempimento un obbligo legale al quale è soggetto il Titolare del trattamento ai sensi dell'art. 6 par. 2 lett. c).

***

Articolo 2 - Norme di riferimento e principi generali

1) Norme di riferimento
    a. Per tutto quanto non dettagliatamente disciplinato nel presente documento, si rinvia a quanto disposto dalle seguenti norme in quanto applicabili:
        - 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 di seguito RGPD)
        - 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*";
        - 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;
        - Decreto Legislativo 18 maggio 2018, n. 51 – Attuazione della Direttiva UE 2016/680 relativa "*alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*";
        - Decreto 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*";
        - Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008);
        - Legge 7 marzo 1986 n. 65 sull'ordinamento della Polizia Locale;
        - D.L. 23 maggio 2008, n. 92, recante "Misure urgenti in materia di sicurezza pubblica", convertito in legge 24 luglio 2008 n. 125;
        - Legge n. 38/2009 recante "misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori".

- Circolare dell'11 settembre 2020 - Disposizioni urgenti in materia di sicurezza delle città, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48. Patti per l'attuazione della sicurezza urbana e installazione di sistemi di videosorveglianza
- Art. 54 del D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni;
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati (European Data Protection Board);
- Art.5 del decreto-legge 20 febbraio 2017, n.14 convertito con modificazioni dalla legge 18 aprile 2017, n.48.

b. I dati personali raccolti per l'esecuzione di un compito di sicurezza pubblica effettuato dall'autorità competente per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali sono trattati nel rispetto dei principi dell'art.3 del D.lgs. 51/2018, ed in particolare:
   - per le limitazioni alla raccolta dei dati e per la loro cancellazione si applica l'art. 12 del D.lgs. 51/2018;
   - per il diritto di accesso ai dati ed alle immagini personali si applica l'art. 11 del D.lgs. 51/2018;
   - per la conservazione dei dati si applica l'art. 4 del D.lgs. 51/2018.

c. I dati personali raccolti per l'esecuzione compiti di interesse pubblico o connessi all'esercizio di pubblici poteri diversi da quelli del punto precedente di cui è investito il Titolare del trattamento sono trattati nel rispetto dei principi dell'art.5 del Reg. UE/2016/679, e:
   - per le limitazioni alla raccolta dei dati e la loro cancellazione sono applicati gli articoli 18 e 17 del Reg. UE/2016/679.
   - per il diritto di accesso ai dati ed alle immagini personali l'art. 15 del Reg. UE/2016/679.

2) Principi generali

L'utilizzo dei sistemi della videosorveglianza viene nel rispetto dei principi applicabili al trattamento di dati personali di cui all'art. 5 dell'RGPD:

a. liceità, quale rispetto della normativa: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è effettuato esclusivamente per scopi determinati ed espliciti. Esso, infatti, è necessario per l'adempimento un obbligo legale al quale è soggetto il Titolare del trattamento nonché per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui il Comune e il Comando di Polizia Locale di Buttigliera Alta sono investiti.

b. proporzionalità e non eccedenza: nel commisurare la necessità del sistema di videosorveglianza al 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 una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare

parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento;

c. Minimizzazione: I dati trattati mediante il sistema di videosorveglianza sono limitati a quelli necessari per il perseguimento delle finalità specifiche dichiarate.

***

Articolo 3 – Definizioni

1) Ai fini del presente regolamento, si intende:

   a. per il "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;

   b. 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;

   c. "Titolare del trattamento" è il Comune nella persona del Sindaco *pro tempore*, cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali;

   d. "responsabile interno" (soggetto designato), la persona fisica, legata da rapporto di servizio al Titolare, che opera sotto la sua autorità e designata dal medesimo allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali ai sensi dell'art. 2-quaterdecies del D.lgs. 196/2003 come mod. dal D.lgs. 101/2018;

   e. "Responsabile del trattamento" ai sensi dell'art. 28 GDPR è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che tratta dati personali per conto del Titolare del trattamento;

   f. per "autorizzati", le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile del Trattamento ai sensi degli artt. 29 del GDPR e 2 *quaterdecies* del D.lgs. 196/2003 come mod. dal D.lgs. 101/2018;

   g. per "interessato", la persona fisica che può essere identificata o identificabile, a cui si riferiscono i dati personali;

   h. per "comunicazione", l'operazione consistente nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione e/o consultazione;

   i. per "diffusione", l'operazione consistente nel dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

j. per "dato anonimo", il dato soggetto a procedura di "anonimizzazione", ovvero il risultato del trattamento di dati personali volto a impedire irreversibilmente l'identificazione del soggetto a cui gli stessi si riferiscono.;

k. per "limitazione", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

Per ogni ulteriore definizione non compresa nell'elenco di cui sopra, si rinvia inoltre a quanto previsto dall'art. 4 del RGPD.

***

Articolo 4 - Finalità degli impianti

1) Il sistema di videosorveglianza è finalizzato a tutelare la sicurezza pubblica e urbana, così come definite e richiamate, rispettivamente, dall'articolo 6 della legge 38/2009, dal D.lgs. 51/2018, dal Decreto del Ministero dell'Interno del 05/08/2008 e dal Decreto Legge 20 febbraio 2017 n. 14, ed a concorrere alla tutela della sicurezza integrata in collaborazione con le forze di polizia dedicate.

2) Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono relative alle funzioni istituzionali demandate ai Sindaci ed ai Comuni:

   a. dal decreto-legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 "*disposizioni urgenti in materia di sicurezza delle città*";

   b. dal D.lgs. 18 agosto 2000, n. 267, dal D.P.R. 24 luglio 1977, n. 616;

   c. dalla legge sull'ordinamento della Polizia Locale 7 marzo 1986, n. 65 nonché dallo Statuto Comunale e dai Regolamenti Comunali vigenti.

   Nello specifico, tali finalità sono dirette a:

   a. attivare misure di prevenzione e sicurezza sul territorio Comunale;

   b. assicurare la protezione e l'incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e sicurezza pubblica, la prevenzione, accertamento o repressione dei reati o esecuzione di sanzioni penali a norma del D.lgs. 51/2018;

   c. promuovere uno strumento operativo di Protezione Civile sul territorio comunale;

   d. controllare il traffico veicolare al fine di prevenire problemi inerenti alla viabilità;

   e. tutelare l'integrità del patrimonio immobiliare e mobiliare del Comune di Buttigliera Alta da atti vandalici e danneggiamenti;

   f. controllare aree pubbliche o aperte al pubblico in occasione di eventi a rilevante partecipazione di pubblico;

   g. ricostruire, ove possibile, la dinamica degli incidenti stradali;

   h. gestire le attività di rilevazione, prevenzione e controllo delle infrazioni, nel quadro delle competenze attribuite dalla legge;

   i. acquisire di fonti di prove in ambito delle attività di polizia amministrativa;

j. vigilare sulle situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;

k. monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;

l. verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;

3) Tra le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono espressamente escluse quelle definite dall'art. 4 dello Statuto dei lavoratori (legge 300 del 20 maggio 1970) relative al controllo a distanza dell'attività dei lavoratori per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

***

Articolo 5 - Caratteristiche tecniche

1) Per il raggiungimento delle finalità istituzionali di cui al precedente articolo, può essere utilizzata, nei limiti imposti da leggi e regolamenti, ogni tecnologia di videosorveglianza e ripresa video e di captazione di immagini, quali:

- telecamere fisse e mobili;
- body-cam (sistemi di ripresa indossabili) e dash-cam (telecamere a bordo veicoli di servizio);
- sistemi aeromobili a pilotaggio remoto (droni);
- videosorveglianza partecipata;

nel rispetto della normativa vigente e delle caratteristiche tecniche e di sicurezza previste dal presente regolamento.

2) In conformità alle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video pubblicate dal Comitato europeo per la protezione dei dati (European Data Protection Board), le caratteristiche tecniche dell'impianto di videosorveglianza devono essere adeguate ed improntate a garantire la sicurezza logica e fisica, mediante l'attuazione di misure tecniche ed organizzative idonee a tutelare:

a. la sicurezza e l'integrità fisica di tutti i componenti del sistema, intesa quale protezione e resilienza in caso di
    - interferenze volontarie e involontarie nel suo normale funzionamento;
    - furti, atti vandalici, calamità naturali, eventi provocati dall'uomo e danni accidentali;
    - accessi logici e fisici al sistema da parte di soggetti non autorizzati.

b. la sicurezza dei dati, ovvero la riservatezza (i dati sono accessibili esclusivamente a soggetti autorizzati), l'integrità (prevenzione della perdita o della manipolazione dei dati) e la disponibilità (i dati possono essere consultati ogniqualvolta sia necessario).

3) La sicurezza del sistema e dei dati, intesa quale protezione dei dati da interferenze volontarie e involontarie nel suo normale funzionamento, può includere le seguenti misure:

- la protezione dell'intera infrastruttura del sistema di videosorveglianza (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti;
- la protezione della trasmissione di filmati mediante canali di comunicazione sicuri;
- la cifratura dei dati;
- l'utilizzo di soluzioni hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;
- l'utilizzo di sistemi rilevamento di guasti di componenti, software e interconnessioni;
- l'utilizzo di procedure e/o strumenti per ripristinare la disponibilità dei dati personali e l'accesso agli stessi in caso di interruzioni e/o malfunzionamenti.

4) Le procedure di controllo degli accessi devono essere in grado di garantire l'accesso al sistema e ai dati esclusivamente ai soggetti autorizzati. Le misure di sicurezza che attuano il controllo fisico e logico degli accessi includono:
   a. la sicurezza fisica dei locali in cui vengono conservati i dispositivi di monitoraggio e videoregistrazione (monitor e VDR);
   b. il posizionamento dei monitor in modo tale da consentire la visualizzazione ai soli soggetti autorizzati;
   c. la definizione e l'applicazione delle policy e procedure per la concessione, la modifica e la revoca delle credenziali di accesso al sistema agli utenti autorizzati;
   d. l'attuazione di metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui l'attribuzione di credenziali personali per ciascun autorizzato, la lunghezza e la complessità delle password e la frequenza della loro modifica;
   e. procedure di registrazione e conservazione dei file di log di accesso degli utenti al sistema e ai dati;
   f. procedure di monitoraggio del sistema finalizzate all'individuazione di guasti e/o malfunzionamenti e la risoluzione in tempi brevi delle carenze individuate.

***

Articolo 6 – Installazione e successive implementazioni dei sistemi di videosorveglianza

1) Ai fini dell'installazione di un impianto di videosorveglianza, sia fisso che mobile, nell'ambito del territorio del Comune di Buttigliera Alta, viene adottata la seguente procedura:
   a. Il Responsabile dei lavori pubblici, dotandosi del supporto tecnico necessario, predisporrà il progetto tecnico che individuerà puntualmente tutte le componenti tecniche del nuovo sistema di videosorveglianza e le misure tecniche ed organizzative che saranno adottate per la sicurezza dei dati personali trattati. Nei casi di impianti con punti ripresa fissa, il progetto indicherà in dettaglio i punti di installazione e la zona oggetto di ripresa delle telecamere, mentre in caso di punti di ripresa mobili indicherà i criteri da rispettare per l'individuazione dei punti e delle modalità di ripresa.
   b. La Giunta attraverso apposita delibera approverà i siti di ripresa e/o i criteri guida da adottare per individuare i punti e le modalità di ripresa in caso di punti di ripresa mobili.

c. A seguito dell'approvazione della Giunta delle specifiche di cui al precedente punto, il Titolare del trattamento, mediante il necessario supporto tecnico e, ove necessario, con il parere del DPO, effettuerà la DPIA.

d. Qualora all'esito della valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 dell'RGPD, considerate le tipologie di sistemi adottati e nonostante le misure tecniche ed organizzative poste in essere, residui un rischio elevato per i diritti e le libertà degli interessati, il Titolare del trattamento, prima di procedere al trattamento, consulterà l'autorità di controllo (Garante protezione dei dati personali) secondo quanto previsto dall'art. 36 del RGPD.

2) Per l'implementazione impianto di videosorveglia già in uso del Comune viene adottata la seguente procedura:

a. Il Responsabile dei lavori pubblici, dotandosi del supporto tecnico necessario, predisporrà il progetto tecnico che individuerà puntualmente tutte le modifiche necessarie alle componenti tecniche del nuovo sistema di videosorveglianza e alle misure tecniche ed organizzative adottate per la sicurezza dei dati personali trattati. Nei casi di impianti con punti ripresa fissa, il progetto, indicherà in dettaglio i punti di installazione e le zone oggetto di ripresa delle telecamere che verranno eliminate, spostate o aggiunte, mentre in caso di punti di ripresa mobili indicherà le eventuali modifiche ed i criteri che dovranno essere attuati per individuare i punti e le modalità di ripresa.

b. La Giunta attraverso apposita delibera approverà la nuova configurazione di siti di ripresa e/o le eventuali modifiche ai criteri che dovranno essere attuati per individuare i punti e le modalità di ripresa.

c. A seguito dell'approvazione della Giunta dei punti e dei criteri, il Responsabile dei lavori pubblici:

- In caso di modifiche significative, mediante il necessario supporto tecnico e, ove necessario, con il parere del DPO, effettuerà la DPIA. A seguito del buon esito della DPIA (rischio residuo accettabile) il Responsabile attuerà le normali procedure adottate dal Comune per l'acquisto, l'installazione e la messa in esercizio del nuovo impianto di videosorveglianza.
- In caso di modifiche di lieve entità e/o comunque tali da non comportare un impatto significativo sulla la validità della DPIA precedentemente effettuata, previo parere del DPO, attuerà direttamente le normali procedure adottate dal Comune per l'acquisto, l'installazione e la messa in esercizio del nuovo impianto di videosorveglianza.

***

Articolo 7 – Il deposito dei rifiuti

1) In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di telecamere risulta consentito 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 qualora non risulti possibile, o si riveli inefficace, il ricorso a strumenti e sistemi di controllo alternativi.

2) Analogamente, l'utilizzo di telecamere 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).

3) Per tali finalità, nel rispetto dei principi espressi nel presente Regolamento, potranno anche essere utilizzati telecamere di tipo riposizionabile o modulari (fototrappole). Il trattamento dei dati personali effettuato mediante l'uso di telecamere per le finalità di cui ai precedenti commi 1 e 2, costituisce trattamento di dati personali e non forma oggetto di disciplina specifica; al riguardo si applicano pertanto le disposizioni generali in tema di protezione dei dati personali e quelle del presente regolamento.

***

Articolo 8 - Dispositivi elettronici per la rilevazione di violazioni al Codice della Strada

1) È consentito l'utilizzo di impianti elettronici di rilevamento delle violazioni al Codice della Strada, nel rispetto della normativa di riferimento. Tali sistemi fotografano le targhe ciascun mezzo in transito nell'area oggetto di rilevamento e - eventualmente mediante l'ausilio di un software integrato OCR - ne leggono il contenuto estraendo la stringa di caratteri alfanumerici. I files che documentano l'illecito (video, fotogrammi) vengono salvati nella memoria del dispositivo di rilevamento in forma criptata e sono accessibili esclusivamente dalla Polizia locale.

2) I dati raccolti mediante tali sistemi sono limitati al perseguimento delle finalità istituzionali del titolare. È necessario limitare la dislocazione e l'angolo visuale delle riprese in modo da omettere immagini non pertinenti e/o ultronee.

3) Nello specifico:

   a. gli impianti elettronici di rilevamento consentono la conservazione dei dati alfanumerici delle targhe automobilistiche nei soli casi in cui emerga una violazione delle disposizioni in materia di circolazione stradale. Per quanto concerne gli impianti dotati di software OCR, che rilevano ogni singolo veicolo in transito, la cancellazione delle targhe dei veicoli esenti da infrazioni verrà processata automaticamente entro 7 giorni dal rilevamento.

   b. le risultanze fotografiche e/o le riprese video acquisiscono esclusivamente 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); escludendo, per quanto possibile, ulteriori dati che coinvolgano soggetti estranei all'accertamento amministrativo (es., pedoni, altri utenti in circolazione);

   c. le risultanze fotografiche o le riprese video rilevate sono utilizzate esclusivamente 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;

   d. le immagini sono 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;

e. le fotografie o le immagini, che costituiscono fonte di prova per le violazioni contestate, non verranno inviate d'ufficio al domicilio del proprietario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;

f. in considerazione del legittimo interesse del proprietario del veicolo di verificare l'autore della violazione, la documentazione videofotografica verrà resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, saranno opportunamente oscurati e/o resi non riconoscibili i passeggeri eventualmente presenti a bordo del veicolo.

***

Articolo 9 - Strumenti diversi di rilevazione immagini: Body-Cam e Dash-Cam

1) Per i servizi a maggior rischio operativo, gli operatori di Polizia Locale possono utilizzare, delle body-cam (telecamere installate sul corpo dell'operatore in servizio) e delle dash-cam (telecamere a bordo dei veicoli di servizio), in conformità con le indicazioni dettate dal Garante della Privacy con nota del 30/9/2014, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi. In tali casi il trattamento dati 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".
2) Il Comando di Polizia Locale curerà la predisposizione di uno specifico disciplinare tecnico interno, da somministrare agli operatori che saranno dotati di microcamere, con specificazione dei casi in cui le microcamere stesse devono essere attivate, dei soggetti autorizzati a disporre l'attivazione, delle operazioni autorizzate in caso di emergenza e di ogni altra misura organizzativa e tecnologica necessaria alla corretta e legittima gestione di detti dispositivi e dei dati trattati.
3) Le video camere e le schede di memoria di cui sono dotati i sistemi di cui al comma 1 dovranno essere contraddistinte da un numero seriale che dovrà essere annotato in apposito registro recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del dipendente che firmerà la presa in carico e la restituzione. La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato. Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte al comma 1.
4) Il trattamento dei dati personali effettuati con simili sistemi di ripresa devono rispettare i principi del Codice Privacy richiamati nel presente regolamento 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.

***

Articolo 10 - Altri strumenti di rilevazione immagini: droni

1) Il Comando di Polizia Locale per lo svolgimento delle attività di competenza può dotarsi di ogni altra tecnologia di ripresa video e captazione di immagini necessaria al raggiungimento delle

finalità istituzionali. In particolare può dotarsi di Sistemi Aeromobili a Pilotaggio remoto – droni – per l'esecuzione di riprese esclusivamente per finalità di prevenzione volte alla tutela di specifici e contestuali motivi di sicurezza urbana nonché per attività di prevenzione, indagine e perseguimento di reati. In ogni caso, i dispositivi ed il loro utilizzo devono essere conformi alla normativa vigente, con particolare riferimento alla regolamentazione adottata dall'Ente Nazionale per l'Aviazione Civile e al Codice della Navigazione.

2) Le modalità di impiego di tali dispositivi in questione saranno disciplinate con apposito provvedimento del Comando di Polizia Locale e gli stessi dovranno essere utilizzati da personale abilitato. In ogni caso le modalità di trattamento e di conservazione dovranno rispettare quanto indicato dal presente regolamento nonché quanto disposto dalla vigente normativa.

***

Articolo 10bis - Altri strumenti di rilevazione immagini: videosorveglianza partecipata

1) Al fine di rafforzare le azioni di prevenzione e contrasto ai fenomeni di illegalità presenti sul territorio, il Comune di Buttigliera potrà adottare sistemi partecipati di videosorveglianza delle aree pubbliche (c.d. videosorveglianza partecipata) nel rispetto dei principi di cui al presente Regolamento e secondo i limiti e le condizioni imposte dalle leggi applicabili, in particolare in materia di protezione dei dati personali.

2) La videosorveglianza partecipata è un progetto che consiste nell'adozione di soluzioni tecnologiche che permettano l'integrazione tra i sistemi di videosorveglianza comunale con quelli dei privati (persone fisiche o giuridiche) che si rendano disponibili a condividere infrastrutture e telecamere proprie per finalità di sicurezza pubblica e controllo del territorio.

3) La Giunta, attraverso appositi atti successivi, provvederà a definire le condizioni e le modalità di adesione dei privati al progetto di videosorveglianza partecipata, le specifiche tecniche degli impianti, le modalità d'individuazione dei punti ripresa, le misure di sicurezza dei canali di comunicazione tra sistemi ed ogni altro requisito necessario all'efficace attuazione del progetto.

***

Articolo 11 – Compiti e responsabilità

1) GIUNTA COMUNALE

La Giunta comunale con apposito atto individua la dislocazione sul territorio comunale i punti dove sono collocate le telecamere nel rispetto delle regole disciplinate dal presente regolamento, individua anche i locali dove destinati ad ospitare le apparecchiature relative alla videosorveglianza.

2) TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati è il Comune, al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

Il Titolare del trattamento, tenuto conto della natura, del contesto e della finalità del trattamento, deve garantire, ed essere in grado di dimostrare, che il trattamento è effettuato non solo in maniera conforme alla normativa ma in maniera tale da non determinare rischi e quindi di non gravare sui diritti e le libertà degli interessati.

3) RESPONSABILE INTERNO (DESIGNATO)
(soggetto designato ai sensi dell'art. 2-quaterdecies D.lgs. 196/2003)

Il Responsabile della Polizia Municipale è designato, ai sensi del Art. 2-quaterdecies D.lgs. 196/2003, quale soggetto con specifici compiti e funzioni con il profilo di Responsabile interno del trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza.

Il Responsabile interno del trattamento è tenuto a conformare il proprio operato nel pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente regolamento.

Il Responsabile interno procede al trattamento dei dati attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

Il Titolare del trattamento, oltre alla figura del Responsabile interno, individua e nomina mediante specifici atti di autorizzazione ulteriori soggetti interni (autorizzati) impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni dell'RGPD; detti soggetti autorizzati sono opportunamente istruiti e formati dal Titolare del trattamento e dal Responsabile interno con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative porre in essere per ridurre i rischi connessi alle ipotesi di trattamento non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati personali.

Il Responsabile interno 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.

Il Responsabile interno è responsabile dell'accesso e della sicurezza delle centrali di controllo, degli apparati hardware e dei software.

Il Responsabile interno conserva ed è responsabile della conservazione delle chiavi e di eventuali altri disposti per l'accesso ai locali della sala di controllo, degli armadi per la conservazione degli eventuali supporti di archiviazione digitale e di ogni altro supporto informatico.

Essendo l'accesso ai dati consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione (password), per assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento di una incaricato/addetto il Responsabile interno è il Custode delle copie delle credenziali.

Trattandosi di dati particolari le persone ammesse a qualunque titolo alle registrazioni devono essere identificate e registrate, il Responsabile interno rilascia autorizzazione per la visione

dei dati registrati da parte dell'Incaricato/addetto ed è responsabile della tenuta di un apposito Registro degli accessi (anche elettronico), nel quale sono riportati ad opera degli Incaricati/addetti almeno i seguenti dati:

- un identificativo dell'Incaricato/addetto
- la data e l'ora dell'accesso;
- i dati per i quali si è svolto l'accesso;
- la motivazione dell'accesso;

4) RESPONSABILE DEL TRATTAMENTO
(ai sensi dell'art. 28 dell'RGPD)

Il responsabile del trattamento, ai sensi dell'art. 28 del RGPD, è la ditta installatrice e responsabile della manutenzione dell'impianto.

Il Titolare può nominare, qualora si rilevi la necessità, altri responsabili esterni ai sensi dell'art. 28 del RGPD.

I rapporti con i responsabili esterni, ai sensi dell'art. 28 del RGPD, sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli stati membri.

5) SOGGETTI AUTORIZZATI AL TRATTAMENTO

a. Ai sensi dell'art. 2-quaterdecies D.lgs. 196/2003, il Titolare autorizza al trattamento dei dati personali le persone che operano sotto l'autorità del Titolare nell'ambito degli Agenti di Polizia Locale. Al soggetto autorizzato verranno affidate specifiche e personali credenziali di accesso al sistema nonché le chiavi della sala di controllo e dell'armadio destinato alla conservazione dei supporti magnetici. L'autorizzato dovrà trattare i dati personali attenendosi scrupolosamente alle istruzioni del Titolare o del responsabile interno.
b. Fatte salve le ipotesi di esercizio dei diritti degli interessati ai sensi degli artt. 15-22 del RGPD nonché in caso di esercizio del diritto di, I dati oggetto di registrazione possono essere riesaminati, a seguito di regolare autorizzazione richiesta al Responsabile interno del trattamento dei dati personali designato e previa compilazione di tutti i dati previsti dal Registro degli accessi e nel limite del periodo di conservazione di cui all'art. 12 paragrafo 1, solo in caso di effettiva necessità ed in relazione alle finalità di cui all'art. 4 del presente regolamento.
c. 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 di eventuali procedimenti penali.

***

Articolo 12 - Valutazione di Impatto sulla protezione dei dati (DPIA)

1) Posto che il trattamento di dati personali effettuati mediante sistemi di videosorveglianza rispondono alla definizione di "*sorveglianza sistematica su larga scala di una zona accessibile al pubblico*", e come tale rientra tra le ipotesi soggette a valutazione di impatto ex art. 35 del

RGPD (cd. DPIA) così come disposto dall'Autorità Garante per la protezione dei dati personali (Cfr. Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018), l'Ente, seguendo la relativa procedura, effettuerà la valutazione di impatto sulla protezione dei dati personali prima della messa in esercizio degli impianti e di ogni successiva implementazione degli stessi.

2) Ai sensi dell'art. 35, paragrafo 2, l'Ente, in occasione dell'esecuzione della valutazione d'impatto, il Titolare del trattamento si consulterà con il responsabile della protezione dei Dati (DPO), in quanto soggetto deputato a fornire, se richiesto, un parere in merito alla valutazione stessa e sorvegliarne lo svolgimento. Nel caso in cui il Titolare non concordi con le indicazioni del DPO dovrà motivare e formalizzare il proprio dissenso.

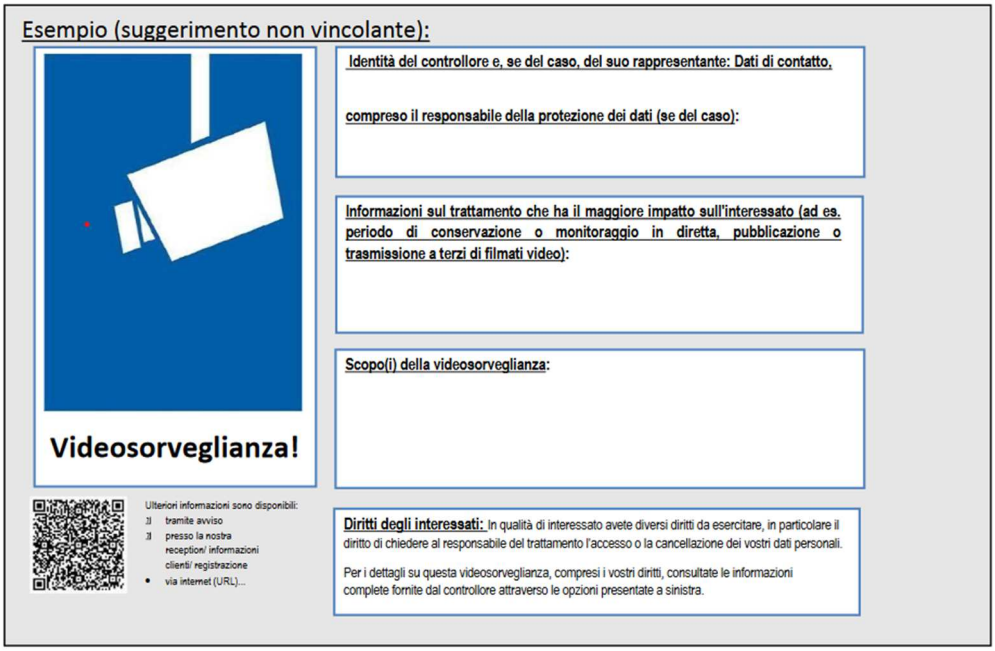
3) Qualora all'esito della valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del RGPD, considerate le tipologie di sistemi adottati e nonostante le misure tecniche ed organizzative poste in essere, residui un rischio elevato per i diritti e le libertà degli interessati, il Titolare del trattamento, prima di procedere al trattamento, consulterà l'Autorità di controllo (Garante protezione dei dati personali) ai sensi dell'art. 36 del RGPD.

***

Articolo 13 – Obblighi informativi e di trasparenza sul trattamento dei dati

1) In conformità alle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video pubblicate dal Comitato europeo per la protezione dei dati (European Data Protection Board) e a quanto disposto degli artt. 13-14 del RGDP, gli obblighi informativi e di trasparenza nel trattamento dei dati personali degli interessati vengono soddisfatti mediante le seguenti soluzioni:
    a. Installazione della segnaletica di avvertimento nei pressi delle telecamere (informativa di primo livello);
    b. pubblicazione di un'informativa completa e di dettaglio sul portale web del Comune di Buttigliera Alta, raggiungibile mediante l'indicazione di un link di rimando (informativa di secondo livello).

2) La segnaletica di avvertimento dovrà:
    a. specificare l'identità del Titolare del trattamento, le finalità del trattamento, l'esistenza dei diritti dell'interessato (le cui modalità di esercizio verranno specificate nell'informativa di secondo livello), la base giuridica e le finalità di del trattamento, i recapiti del responsabile della protezione dei dati, il periodo di conservazione e l'eventuale trasmissione dati a terzi, oltre all'indicazione di un link/QRCode di rimando al portale web del Comune di Buttigliera Alta per consentire la consultazione dell'informativa di secondo livello.
    b. essere posizionata in modo da permettere all'interessato di avere cognizione della presenza dell'impianto di videosorveglianza prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi) e di stimare il perimetro della zona stessa in modo da evitare l'inquadratura e/o adeguare il proprio comportamento, ove necessario.
    c. utilizzare un modello conforme al fac-simile riportato sulle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati (European Data Protection Board) e potrà inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificata al fine di informare se le immagini sono solo visionate o anche registrate;



d. avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

In presenza di più telecamere, in relazione all'estensione dell'area oggetto di rilevamento e alle modalità delle riprese, dovranno essere installati più cartelli.

3) Informativa di secondo livello dovrà essere facilmente accessibile per l'interessato. Oltre l'indicazione di un link di rimando al portale web del Comune di Buttigliera Alta impresso sulla segnaletica di avvertimento, l'informativa verrà resa disponibile in formato analogico presso gli uffici comunali. Indipendentemente dal formato, l'informativa dovrà contenere tutti gli elementi obbligatori previsti dell'art. 13 del RGPD.

4) Per quanto riguarda strumenti di acquisizione specifici, come ad esempio body-cam/dash cam, l'informativa di primo livello è resa verbalmente da parte dell'operatore all'inizio della registrazione, mentre l'informativa di secondo livello sul trattamento dei dati personali ai sensi degli artt. 13-14 del RGDP è verrà resa disponibile attraverso l'indicazione di un link di rimando al portale web del Comune di Buttigliera Alta indicata.

***

Articolo 13 - Modalità di raccolta dei dati personali

1) I dati personali oggetto di trattamento saranno trattati ai sensi dell'art. 5 del RGPD, ovvero:

a. in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del RGPD, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

***

Articolo 14 - Accertamenti di illeciti e indagini di Autorità Giudiziarie o di Polizia

1) Il trattamento di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzionipenali e non sono soggetti al RGPD ma alla Direttiva (UE) 2016/680 e al D.lgs. 81/2018.

2) Il Responsabile interno o il soggetto autorizzato procederà all'acquisizione di immagini e/o di video su supporti digitali mediante misure tecniche atte ad impedirne l'alterazione nei casi in cui:

   a. dovessero essere rilevate immagini costituenti ipotesi di reato o consistenti in eventi rilevanti ai fini della sicurezza pubblica e/o della tutela ambientale e/o del patrimonio, provvedendo a darne immediata comunicazione agli organi competenti;

   b. le Forze di polizia e/o l'autorità giudiziaria nello svolgimento delle proprie funzioni ne facciano richiesta scritta e motivata.

3) L'acquisizione di cui al punto precedente sarà corredata da una completa verbalizzazione delle operazioni svolte in ordine cronologico mediante:

   a. annotazione relativa all'esecuzione del download dei filmati – Nome addetto, data e ora;

   b. annotazione relativa alla visione dei filmati – Nome addetto, data e ora;

   c. annotazione dei fatti salienti relativi all'evento rilevato – Nome addetto, data e ora;

   d. annotazione relativa alle operazioni di salvataggio dei filmati e dei supporti di memorizzazione utilizzati – Nome addetto, data e ora;

   e. annotazione circa alle eventuali estrapolazioni di fotogrammi per comporre fascicoli fotografici esplicativi per l'imitare l'accesso documentale ai filmati – Nome addetto, data e ora.

4) Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di Polizia Giudiziaria e l'Autorità Giudiziaria.

***

Articolo 15 - Sicurezza dei dati

1) I sistemi di videosorveglianza sono protetti da idonee misure di sicurezza fisica e logica atte a ridurre al minimo i rischi di accesso non autorizzato, distruzione, modifica, perdita, ancorché accidentale, dei dati.

2) I videoregistratori digitali nonché gli ulteriori supporti di memorizzazione deputati alla registrazione e conservazione delle immagini sono custoditi nella sala di controllo ubicata all'interno degli edifici Comunali;

3) Le sale di monitoraggio video sono ubicate, rispettivamente, nella Sede Comunale e presso il Comando della Polizia Locale. L'accesso alle sale è costantemente presidiato e protetto da adeguate misure di sicurezza atte a consentirne l'accesso ai soggetti autorizzati ai sensi dell'art. 11 nonché alla ditta manutentrice del sistema, quest'ultima in qualità di soggetto Responsabile del trattamento ai sensi dell'art. 28 del GDPR;

4) Il Responsabile interno è il soggetto deputato alla sicurezza fisica dell'impianto e al controllo degli accessi alla sala di controllo. A tal proposito il Responsabile interno provvede a mantenere apposito registro degli accessi.

5) I Il sistema di videosorveglianza garantisce la registrazione degli accessi logici (data, ora, operatore) che vengono conservati appositi file di log che per un periodo di 60 gg. I file di log applicano misure di sicurezza e protezione atte ad evitare manomissioni ed accessi non autorizzati.

***

Articolo 16 - Accesso ai dati

1) L'accesso ai dati registrati al fine della consultazione ed analisi, nel rispetto del periodo di conservazione di cui al punto 11, è consentito esclusivamente in caso di effettiva necessità e nel limite delle finalità di cui all'art. 4 del presente regolamento.

2) L'accesso alle immagini è consentito esclusivamente:

   a. al Responsabile interno ed agli autorizzati al trattamento;

   b. alle Forze di polizia e all'autorità giudiziaria, nello svolgimento delle rispettive funzioni;

   c. al difensore della persona offesa o sottoposta alle indagini, nell'ambito delle investigazioni difensive, a norma dell'art. 391-quater c.p.p.,

   d. ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente.

   e. al soggetto interessato (in quanto oggetto delle riprese) che eserciti il diritto di accesso alle immagini. L'accesso da parte dell'interessato sarà limitato alle sole immagini che lo riguardano direttamente con specifica esclusione di fotogrammi che rappresentino ulteriori soggetti estranei alla richiesta;

   f. ai soggetti di cui al precedente art. 11 del presente regolamento.

   L'accesso alle immagini, nei casi di cui alle precedenti lettere a), c) e d) potrà avvenire solo ed esclusivamente previa specifica richiesta motivata al Titolare del trattamento e, ad eccezione per quanto previsto dall'art. 12 par. 5 lett. b) del RGPD ed in relazione alle richieste pervenute

dagli organi di Polizia e dall'Autorità Giudiziaria, previa corresponsione delle spese per il rilascio di copia digitale. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione generale, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre forze di polizia, deve essere oggetto di specifici accordi, in cui vengono disciplinati le modalità di accesso, gli ambiti di utilizzo e le correlate responsabilità ai sensi dell'art. 5 del decreto legge 20 febbraio 2017, n. 14 convertito con modificazioni dalla legge 18 aprile 2017, n. 48.

***

Articolo 17 - Periodo di conservazione dei dati

1) Ai sensi dell'art. 6 comma 8 del D.L. 23.02.2009 n. 11 ed in accordo al par. 3.4.3. del Provvedimento del Garante per la protezione dei dati personali del 08.04.2010, il periodo massimo di conservazione delle immagini videoregistrate è limitato ai 7 (sette) giorni successivi alla "*registrazione delle immagini raccolte mediante l'uso di sistemi di videosorveglianza*";
2) Qualora, in base a esigenze specifiche del caso in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti (come ad esempio in caso di specifiche attività investigative in corso), risultasse necessario procedere alla conservazione per un periodo superiore ai 7 giorni, il Titolare dovrà inoltrare al Garante una richiesta di verifica preliminare, adeguatamente motivata. Esaurito il periodo di conservazione dei dati, gli stessi vengono cancellati da ogni supporto medianti tecniche idonee ad impedirne il recupero.

***

Articolo 18 - Diritti dell'interessato

1) Il soggetto interessato può esercitare nei confronti del Titolare del trattamento i diritti previsti dagli artt. 15, 16, 17, 18, 19, 21, 22 del RGPD.
2) L'interessato ha il diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, la loro comunicazione in forma intelligibile e la possibilità di effettuare reclamo presso l'Autorità di controllo.
3) L'interessato ha diritto di ottenere l'indicazione:
   a. dell'origine dei dati personali;
   b. delle finalità e modalità del trattamento;
   c. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d. degli estremi identificativi del Titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2 dell'RGDP;
   e. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati/addetti.
4) L'interessato ha diritto di ottenere:
   a. l'aggiornamento, la rettifica ovvero, quando vi ha interesse, l'integrazione dei dati;

b. 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;

c. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

5) L'interessato ha diritto di opporsi, in tutto o in parte:

a. per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

L'interessato potrà esercitare i diritti sopra elencati mediante richiesta da inviare all'indirizzo email privacy@comune.buttiglieraalta.to.it. Tale richiesta verrà processata dalla persona all'uopo autorizzata.

Il Titolare provvederà a confermare la ricezione della richiesta e a fornire le informazioni relative all'azione intrapresa, con riferimento all'esercizio dei suoi diritti previsti negli articoli da 15 a 22 del GDPR, entro 1 (uno) mese dal ricevimento della richiesta stessa. Se necessario, e tenuto conto della complessità e del numero delle richieste, il Titolare potrà prorogare tale termine di 2 (due) mesi, previa comunicazione motivata da trasmettersi entro 1 (uno) mese dal ricevimento della richiesta.

Il Titolare provvederà a comunicare l'eventuale rettifica, cancellazione, limitazione opposizione a tutti i destinatari, come individuati dall'art. 4, paragrafo 1, n. 9 del GDPR, a cui tali dati sono stati trasmessi, salvo che ciò si riveli impossibile e/o implichi uno sforzo sproporzionato.

A seguito dell'invio della richiesta di rettifica, cancellazione, limitazione opposizione da parte dell'interessato, qualora il Titolare nutra ragionevoli dubbi circa l'identità del medesimo, provvederà a richiedere ulteriori informazioni per confermarla.

Nel caso in cui il Titolare non ottemperi alla richiesta dell'interessato entro il termine di 1 (uno) mese dal ricevimento della richiesta, il Titolare lo informerà dei motivi dell'inottemperanza e della facoltà di proporre reclamo all'Autorità di Controllo (Garante per la protezione dei dati personali), come specificato ai sensi dell'art. 13, paragrafo 2, lettera (d) e disciplinato dagli articoli 77 e ss. del GDPR.

***

Articolo 19 – Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

1) In relazione al diritto di proporre reclamo 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. dell'RGPD ed alle previsioni del D.lgs. 196/2003.

***

Articolo 20 - Pubblicità del regolamento

1) Copia del presente regolamento sarà pubblicata all'Albo Pretorio online e potrà essere reperita sul sito internet del Comune nella sezione Amministrazione Trasparente - Atti generali.

***

Articolo 21 – 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.