COMUNE DI JESOLO

Regolamento per l'esercizio del sistema di videosorveglianza del Comune di Jesolo,

aggiornato al Reg. UE 2017/679 – GDPR, al D.Lgs. 51/2018 e al D.Lgs.101/2018

Titolo documento:	**Regolamento per l'esercizio del sistema di videosorveglianza del Comune di Jesolo**
Codice documento:	Jesolo – REGVDS-12-0
Nome file:	Jesolo – REGVDS Ver 12-0
Stato documento:	Prima emissione ufficiale
Versione:	12.0
Data ultimo aggiornamento	25 ottobre 2019

Indice

Art. 1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del Reg. UE 2016/679 – GDPR (per brevità nel seguito detto anche semplicemente "*Regolamento"* o "*GDPR*").

Ai sensi dell'art. 4 del Regolamento si intende per:

1) «dati personali»: qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con 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 dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica;

2) «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;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «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;

5) «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 i dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «autorità competente»:

a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o

b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;

8) «titolare del trattamento»: l'autorità competente 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 dello Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione o dello Stato membro;

9) «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;

10) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o dello Stato membro non sono considerate destinatari; il trattamento di tali dati da parte di tali autorità pubbliche è conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento;

11) «violazione dei dati personali»: la violazione della 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;

12) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

13) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

14) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

15) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 41;

16) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art. 2 - Obiettivo del presente Regolamento

Obiettivo del presente regolamento è assicurare che i trattamenti di dati personali effettuati dal Comune di Jesolo nel territorio del Comune di Jesolo mediante il sistema di videosorveglianza, avvengano correttamente, lecitamente, e conformemente a quanto previsto dalla disciplina rilevante in materia di sicurezza e protezione dei dati personali; in particolare, il rispetto del presente regolamento garantirà la conformità:

- al Regolamento UE 2016/679 - GDPR
- alle prescrizioni del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali), così come modificato dal D.Lgs. 101/2018;
- al D.Lgs. 51/2018, relativamente all'utilizzo che può venire fatto del sistema di videosorveglianza per lo svolgimento di attività ed indagini di Polizia Giudiziaria;
- ai provvedimenti del Garante per la protezione del dati personali, con particolare riferimento al provvedimento generale del 8 aprile 2010 del Garante per la protezione dei dati personali, dedicato alla videosorveglianza;
- a quanto previsto da eventuali Regolamenti Comunali relativi alla gestione dei rifiuti solidi urbani;
- ai principi di:
    - liceità;
    - necessità;
    - finalità;
    - non eccedenza e proporzionalità rispetto alle finalità;
    - minimizzazione dei dati.

Art. 3 - Ambito di validità e di applicazione del presente regolamento

Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali e sensibili effettuati mediante sistema di videosorveglianza:

- sotto la **diretta titolarità** del Comune di Jesolo, e
- all'interno del **territorio del Comune di Jesolo**.

In caso di accordi o convenzioni con altri Comuni per il servizio associato di Polizia Locale, anche mediante l'implementazione di collegamenti telematici, ciascun Comune rimarrà comunque autonomo titolare del trattamento dei dati effettuati mediante sistema di videosorveglianza.

Art. 4 - Identificazione del titolare del trattamento dei dati

Il titolare dei trattamenti di dati personali effettuati mediante il sistema di videosorveglianza del Comune di Jesolo è il **Comune di Jesolo** stesso: pertanto, competono esclusivamente al Comune di Jesolo le decisioni in ordine alle finalità e alle modalità del trattamento, compreso anche il profilo della sicurezza. A titolo esemplificativo e non esaustivo, si riportano di seguito alcune decisioni che spettano esclusivamente al Comune di Jesolo:

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

Art. 5 - Obiettivi e finalità del sistema di videosorveglianza

Il sistema di videosorveglianza, in quanto sistema che comporta il trattamento di dati personali, può venire utilizzato esclusivamente per il perseguimento delle funzioni istituzionali del titolare del trattamento dei dati, vale a dire del Comune di Jesolo, nonché per lo svolgimento di attività ed indagini di Polizia Giudiziaria

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

- attivazione di misure di prevenzione e sicurezza sul territorio comunale;
- rilevazione di dati anonimi per l'analisi dei flussi di traffico e per la predisposizione di piani comunali del traffico;
- vigilanza sul pubblico traffico;
- vigilanza (compresa la possibilità di irrogare sanzioni penali e amministrative) sul fenomeno dell'abbandono dei rifiuti;

- raccolta e costituzione di materiale probatorio di natura fotografica e filmica a supporto delle attività di accertamento, contestazione e notificazione di infrazioni, ai sensi degli artt. 13 e 14 della Legge 24 novembre 1981, n. 689;
- raccolta e costituzione di materiale probatorio di natura fotografica e filmica a supporto delle attività di documentazione e comunicazione di notizie di reato;
- svolgimento di attività ed indagini di Polizia Giudiziaria da parte del Corpo di Polizia Locale del Comune di Jesolo, sia su delega oppure attivate di propria iniziativa;
- prevenzione e rilevazione di reati;
- prevenzione e rilevazione di atti vandalici;
- tutela del patrimonio comunale, di beni e di persone;
- rilevazione situazioni di pericolo per la sicurezza urbana, consentendo l'intervento degli operatori;
- rilevazione delle targhe dei veicoli in transito, per le seguenti finalità:
    - rilevazione dei veicoli non assicurati;
    - rilevazione dei veicoli con revisione scaduta;
    - rilevazione dei veicoli rubati;
    - rilevazione dei veicoli smarriti;
    - rilevazione dei veicoli sottoposti a fermo amministrativo
    - rilevazione dei veicoli da tenere sotto controllo, in quanto appartenenti ad una o più "black list";
    - gestione dei veicoli appartenenti a una o più "white list";
- produzione di statistiche e conteggi relativamente alle tipologie di veicoli di cui al punto precedente.

Art. 6 – Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità, e finalità.

6.1 Premessa

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

6.2 Principio di liceità

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

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

6.3 Principio di necessità

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

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

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

casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

6.4 Principio di non eccedenza e proporzionalità

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

- il numero e la collocazione delle telecamere devono essere effettivamente commisurate al reale livello di rischio, evitando la rilevazione o la registrazione in aree che non siano soggette a concreti pericoli o che non siano meritevoli di particolare tutela;
- il posizionamento, la tipologia di telecamere, le aree brandeggiabili, l'utilizzo di zoom, quali dati ed eventi rilevare, devono essere rapportati alle concrete finalità ed esigenze, e si dovranno evitare eccedenze; ad esempio si dovrà limitare la possibilità di brandeggio mediante l'impostazione di vincoli o di mascheramenti statici;
- le telecamere devono essere collocate, e più in generale la videosorveglianza deve essere adottata, solo quando altre misure meno "invasive" siano state ponderatamente valutate insufficienti o inattuabili;
- se l'installazione delle telecamere è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri accorgimenti quali ad esempio controlli da parte di addetti, sistemi di allarme, misure di protezione perimetrale e degli ingressi, abilitazione e controllo degli accessi;
- non è consentita l'installazione meramente dimostrativa o artefatta di telecamere non funzionanti o per finzione, che può essere legittimamente oggetto di contestazione;
- la non eccedenza e proporzionalità deve essere valutata, anche periodicamente, in ogni fase e modalità del trattamento; ad esempio, in fase di definizione e assegnazione dei profili di accesso ai dati, i profili dovranno essere configurati e assegnati in maniera che gli incaricati accedano alla minima quantità di dati necessaria per lo svolgimento dei compiti assegnati; come minimo si dovrà prevedere una fondamentale distinzione tra il profilo di tipo "utente normale" e un profilo più elevato di tipo "administrator";

6.5 Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi, ai sensi dell'art. 5 del GDPR; sono pertanto esclusi utilizzi indeterminati, occulti e non legittimi. In particolare il titolare o il responsabile potranno perseguire solo finalità di propria pertinenza.

Potranno essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività

Polizia Giudiziaria). E non finalità generiche o indeterminate, soprattutto quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti.

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

Art. 7 – Utilizzi esplicitamente vietati

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

Art. 8 – Deposito e abbandono di rifiuti

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

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

E' espliciatamente previsto che il sistema di Videosorveglianza, o un suo sottosistema (come ad esempio le c.d. "***fototrappole***") , possa essere utilizzato per la verifica del rispetto di quanto previsto dalle norme di eventuali Regolamenti emessi dal Comune di Jesolo, per la gestione dei rifiuti solidi urbani.

Art. 9 – 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, quindi al Comune di Jesolo, di richiedere 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. 10 – 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:

a) 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;

b) 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);

c) 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;

d) 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;

e) 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;

f) 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. 11 – Accordi con enti pubblici e privati

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

E' inoltre esplicitamente previsto che il Comune di Jesolo possa stipulare accordi o convenzioni con il soggetto incaricato della gestione dei rifiuti solidi urbani, per disciplinare l'utilizzo dei dipendenti del soggetto gestore nell'attività di accertamento e contestazione di sanzioni amministrative in materia di violazioni della disciplina in materia di smaltimento dei rifiuti, previa designazione dei dipendenti stessi in qualità di "***Ispettori ambientali***" con provvedimento del Sindaco.

Art. 12 – Tipi di trattamenti autorizzati

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

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

- predisposizione delle soglie temporali e degli eventi di cancellazione immagini;
- consultazione immagini registrate;
- estrazione (duplicazione) immagini registrate;
- definizione aree di motion-detection;
- definizione azioni da eseguire in concomitanza di eventi di motion-detection;
- accensione di sorgenti luminose o ad infrarosso;
- attivazione funzionalità di “speak-ip”;
- rilevazione e inventario degli indirizzi ip presenti in rete;
- rilevazione e inventario dei mac address presenti in rete;
- installazione e configurazione di software applicativo;
- installazione e configurazione di software di base;
- installazione di “patch” e “hot fix”;
- attivazione collegamenti da remoto;
- interventi generici di manutenzione e configurazione hardware e software;
- estrazione di files di log;
- conservazione di files di log per un periodo minimo di dodici mesi;
- apposizione di firma digitale qualificata o di codici hash a files di log.

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

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

- Titolare del trattamento dei dati;
- Responsabile della protezione dei dati, ai sensi degli artt. 37, 38 e 39 del GDPR;
- Responsabile esterno del trattamento dei dati: sono i soggetti (persone fisiche o giuridiche) esterni al Comune di Jesolo ai quali sono affidati, da parte del Comune di Jesolo, alcune operazioni di trattamento dei dati e la messa in atto di alcune misure di sicurezza;
- Incaricati del trattamento dei dati: sono i soggetti fisici (persone fisiche) che, designati per iscritto dal titolare o dal responsabile, eseguono una o più operazioni di trattamento dei dati;

- Custode delle password di sistema: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell'amministratore di sistema - delle parole chiave corrispondenti ai vari profili di tipo "administrator" o equivalenti;

- Custode delle parole chiave: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell'incaricato – delle parole chiave assegnate agli utenti finali;

- Soggetti incaricati della gestione e manutenzione degli strumenti elettronici, denominati anche "Amministratori di sistema";

- Altre Pubbliche Amministrazioni che richiedano di accedere ai dati per lo svolgimento delle loro funzioni istituzionali: in questo caso l'accesso e l'utilizzo dei dati messi a disposizione dal Comune di Jesolo, avrà luogo sotto la diretta responsabilità e titolarità della Pubblica Amministrazione o del soggetto richiedente: sarà pertanto cura della Pubblica Amministrazione o del soggetto richiedente verificare che l'accesso avvenga esclusivamente per lo svolgimento delle funzioni istituzionali, e non per il perseguimento di interessi o finalità personali o comunque non chiaramente riconducibili allo svolgimento di funzioni istituzionali o di compiti d'ufficio, senza che vi sia abuso d'ufficio. Sarà inoltre cura della Pubblica Amministrazione o del soggetto richiedente, o del soggetto al quale i dati sono comunicati o portati a conoscenza a seguito di motivata richiesta, mettere in atto quanto previsto dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento all'obbligo di designazione degli incaricati del trattamento, specificando puntualmente per iscritto l'ambito del trattamento consentito e assicurando che le operazioni di trattamento (compresa la mera consultazione, che è comunque una tipologia di trattamento) e l'accesso ai dati avvenga in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Art. 14 – Accesso ai dati da parte delle Forze dell'Ordine e dell'Autorità Giudiziaria

Il D.Lgs. 196/2003, così come modificato dal D.Lgs. 101/2018, prevede che la comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico possa avvenire se:

- prevista da norma di legge o di regolamento, oppure
- anche in assenza di norma di legge o di regolamento, sia necessaria per lo svolgimento delle funzioni istituzionali.

Pertanto le Forze dell'Ordine o l'Autorità Giudiziaria possono lecitamente richiedere di:

- accedere alle immagine "live";
- accedere alle immagini registrate ed ottenete copia delle registrazioni;

- effettuare riprese e registrazioni “ad-hoc”.

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

Le richieste di accesso/estrazioni dovranno seguire le procedure definite nel presente regolamento, ed essere autorizzate dal Sindaco, dal Comandante di Polizia Locale oppure dal Vice Comandante.

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 dall’art. 5 del GDPR e più in generale dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento al provvedimento generale del Garante per la protezione dei dati personali del 8 aprile 2010, dedicato alla videosorveglianza.

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

E’ esplicitamente previsto che i Carabinieri e la Polizia di Stato possano accedere remotamente in via telematica al sistema di Videosorveglianza, per accelerare i tempi di indagine e per sgravare il personale di Polizia Locale del Comune di Jesolo.

Gli accessi dovranno avvenire su base nominativa individuale, e dovranno venire tracciati.

Le modalità di accesso dovranno venire normate con accordo di tipo convenzione o protocollo di intesa.

Art. 15 bis – Accesso telematico da parte di soggetti incaricati di operazioni di assistenza o manutenzione

E’ previsto che per l’effettuazione di alcune operazioni di assistenza e manutenzione da parte di soggetti opportunamente designati in qualità di responsabili esterni del trattamento dei dati ai sensi dell’art. 28 del GDPR, possa avere luogo in modalità “telemanutenzione”, laddove tale prassi sia esplicitamente prevista dai contratti di assistenza.

In ogni caso La gestione della telemanutenzione dovrà soddisfare come minimo i seguenti requisiti di base:

- monitoraggio effettuato tramite protocollo SNMP – Simple Network Management Protocol, che in caso di problemi invia un’e-mail alla ditta incaricata della telemanutenzione che viene letta in orario lavorativo, di tutti gli apparati costituenti il sistema di Videosorveglianza:

- telecamere digitali;

- telecamere ANPR per il riconoscimento delle targhe;
- apparati trasmissivi di rete d'accesso di tipo CPE;
- apparati trasmissivi di dorsale di tipo AP – Access Point;
- apparati trasmissivi di backbone di tipo PTP – Point To Point;
- switch;
- router;
- server e client;
- NAS e apparati di memorizzazione dei dati;
- raid controller;
- impiego dell'ampieza di banda;
- nomi dei dispositivi monitorati;

• accesso remoto e locale limitato alla sola rete del sistema di videosorveglianza: non dovrà essere possibile in nessun modo accedere a reti o sottoreti diverse da quelle usate per il sistema di videosorveglianza;

• accesso remoto effettuato esclusivamente su tratte cifrate, ad esempio mediante VPN;

• identificazione certa dei soggetti che accedono da remoto;

• tracciatura degli accessi e delle operazioni effettuate;

• accesso al sistema di videosorveglianza negoziato ed autorizzato di volta in volta da personale designato per iscritto del Comune di Jesolo.

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

In generale i soggetti coinvolti nelle operazioni di trattamento dovranno essere designati per iscritto dal titolare o dal responsabile del trattamento dei dati, con atto che specifichi chiaramente compiti e responsabilità assegnate. Per quanto riguarda gli incaricati del trattamento dei dati, detti anche "soggetti designati" ai sensi dell'art. 29 del GDPR, oltre ai compiti e alle responsabilità affidate, dovrà essere chiaramente specificato l'ambito del trattamento consentito.

La revisione della sussistenza delle condizioni per il mantenimento dell'ambito del trattamento consentito e del profilo di accesso dovranno essere oggetto di revisione da parte del responsabile o del titolare con frequenza almeno annuale.

Relativamente ai soggetti autorizzati dal Sindaco in qualità di "Ispettore Ambientale", la designazione con atto scritto ad incaricato del trattamento dei dati o di "soggetto designato" ai sensi dell'art. 29 del GDPR, dovrà essere effettuata dal Sindaco con atto scritto.

Art. 17 – Designazione dei "soggetti autorizzati" ai sensi dell'art. 29 del GDPR

Coerentemente con quanto prescritto dal punto 3.3.2. del Provvedimento del Garante per le protezione dei dati personali del 8 aprile 2010, la designazione degli incaricati dovrà avvenire con modalità che permettano di esplicitare con la massima granularità le tipologie di operazioni alle quali ciascun incaricato risulterà essere abilitato. L'ambito del trattamento consentito agli incaricati dovrà inoltre essere oggetto di verifica (ed eventuale modifica) almeno annuale.

La designazione dei soggetti incaricati ed autorizzati dovrà essere effettuata ai sensi dell'art. 29 del GDPR.

Art. 18 – Obblighi degli incaricati/operatori

L'utilizzo delle telecamere è consentito solo per la sorveglianza di quanto è ubicato oppure si svolge nelle aree pubbliche. Fatti salvi i casi di richiesta degli interessati, i dati registrati possono essere riesaminati, nel limite di tempo ammesso dal presente regolamento, solo in caso di effettiva necessità e per l'esclusivo perseguimento delle finalità di cui all'art. 5. In ogni caso, l'estrazione di immagini potrà avvenire solo in caso di richiesta/autorizzazione scritta da parte del Sindaco, del Comandante della Polizia Locale o del Vice Comandante, oppure di richiesta proveniente da altra Pubblica Amministrazione, nei casi in cui l'accesso a immagini registrate sia necessario per lo svolgimento delle funzioni istituzionali. Anche in questo ultimo caso l'accesso/estrazione delle immagini dovrà essere autorizzata dal Sindaco, oppure dal Comandante della Polizia Locale oppure dal Vice Comandante.

Una deroga al punto precedente è costituita dalle telecamere dedicate al monitoraggio del fenomeno dello smaltimento dei rifiuti, nel qual caso l'estrazione delle immagini può essere effettuata dagli incaricati del trattamento dei dati senza necessità di richiesta/autorizzazione alcuna.

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

Art. 19 – Tempi di conservazione delle immagini

I tempi di conservazione dei dati gestiti mediante il sistema di videosorveglianza dovranno tenere conto della tipologia di dati, delle finalità per le quali i dati sono acquisiti e trattati, nonché di eventuali prescrizioni/limiti imposti dalla attuale normativa in materia di videosorveglianza e protezione dei dati personali.

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

Per quanto riguarda i dati acquisiti mediante le telecamere ANPR per la rilevazione delle targhe dei veicoli in transito, che sono costituiti:

- dal fotogramma relativo al passaggio del veicolo;
- dall'informazione testuale relativa alla targa del veicolo in transito, prodotta dal sistema OCR – Optical Character Recognition;
- dai dati reperiti mediante accesso ai vari database (es. Motorizzazione Civile, ANIA, veicoli rubati etc.);

tali dati potranno essere conservati per il tempo strettamente necessario alla attivazione e gestione del procedimento, tenendo conto dei tempi previsti dalla vigente normativi in termini di ricorsi od opposizioni. In ogni caso i tempi di conservazione delle immagini dovranno essere tali da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi e alle finalità per le quali i dati stessi sono stati raccolti o successivamente trattati.

Art. 20 – Luogo e modalità di memorizzazione delle immagini

Fatta eccezione per le telecamere "mobili" dedicate al monitoraggio del fenomeno dello smaltimento dei rifiuti, le immagini riprese dalle telecamere dovranno venire memorizzate in formato elettronico su un unico (o un numero limitato) supporto di memorizzazione di massa centralizzato e ben individuato all'interno di un unico e ben determinato apparato di tipo "server" (può essere comunque fatta salva la necessità di una

memorizzazione “di backup” si un server remoto). Il suddetto server dovrà essere dedicato esclusivamente alla memorizzazione delle immagini registrate dalle telecamere del sistema di videosorveglianza, e non dovrà essere dedicato ad altri scopi. Se non diversamente disposto dal titolare con atto scritto, il server non dovrà essere collegato ad internet, oppure dovrà essere collegato solo in casi e per finalità specifiche e ben individuate, per intervalli di tempo il più possibile contenuti.

Una eventuale deroga al punto precedente è permessa nel caso il sistema di videosorveglianza si basi su una architettura in cloud, nel qual caso le immagini possono essere memorizzate su un server remoto raggiungibile tramite internet, ed eventualmente su un server locale.

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

Relativamente invece alle telecamere dedicate al monitoraggio dello smaltimento dei rifiuti, ad esempio di tipo “***fototrappole***”, è consentita la memorizzazione delle immagini e delle riprese filmiche su apposite schede di memoria “SD” alloggiate all’interno della telecamera, oppure su server ftp al quale le immagini possono essere trasmesse dalla telecamera ad intervalli regolari oppure al verificarsi di determinate tipologie di eventi.

Art. 21 – Criteri e modalità di estrazione delle immagini

L’estrazione delle immagini dovrà avvenire seconda quanto specificato dai seguenti passi operativi:

- viene ricevuta la richiesta di estrazione;
- il Comandante autorizza o meno l’estrazione delle riprese filmiche. Nel caso l’estrazione sia autorizzata:
    - l’addetto alla C.O. provvede ad effettuare l’estrazione delle riprese filmiche
    - vengono predisposte due copie delle sequenze filmiche estratte, di cui una rimane agli atti
    - si effettua la consegna con contestuale redazione del verbale di consegna o nota che deve poi essere trasmessa all’Uff. Polizia Giudiziaria che ne cura l’archiviazione tra le proprie pratiche.

Art. 22 – 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. Come minimo dovranno essere applicati algoritmi di cifratura dotati di robustezza maggiore o uguale a DES (Data Encryption Standard).

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

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

- a livello di software di videosorveglianza, deve essere attivato (ed eventualmente configurato) un meccanismo di logging (tracciatura) delle operazioni di amministrazione e gestione di sistema effettuate con profilo di administrator;
- a livello di software di videosorveglianza, il suddetto file di log non deve essere sovrascritto per un periodo minimo di tre mesi;
- il suddetto file di log non dovrà essere per nessun motivo cancellato, modificato o alterato;
- con frequenza al massimo trimestrale, si dovrà procedere all'estrazione (copia) del suddetto file di log;
- la copia estratta del file di log dovrà essere generata in un formato non modificabile (pdf, tiff o altri formati non modificabili) e firmata digitalmente con certificato digitale emesso da una certification authority trusted di primo livello;
- la copia del file di log firmata digitalmente dovrà essere custodita in un luogo sicuro per un periodo di almeno 12 mesi;
- con frequenza trimestrale si dovrà controllare l'operato degli amministratori di sistema, mediante analisi dei file di log e del registro delle operazioni di amministrazione e gestione di sistema effettuate sul sistema di videosorveglianza; alla conclusione delle operazioni di controllo / verifica dovrà essere redatto apposito verbale e relazione.

Art. 24 – Installazione di nuove telecamere

L'installazione di nuove telecamere dovrà essere autorizzata mediante atto deliberativo di Giunta Comunale. Preventivamente si dovrà verificare che:

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

Art. 25 – Installazione di telecamere mobili

E' esplicitamente prevista la facoltà, da parte del responsabile del Servizio di Polizia Locale, di installare per brevi periodi e a fronte di determinate esigenze (es. contrasto dello spaccio di stupefacenti, prostituzione, monitoraggio del fenomeno dello smaltimento dei rifiuti, etc.) telecamere mobili, senza ottenere l'autorizzazione preventiva da parte del Sindaco e della Giunta Comunale.

Tali telecamere potranno memorizzare i dati in locale, su apposita scheda SD installata a bordo della telecamera.

Art. 26 – Utilizzo di telecamere indossabili

E' esplicitamente prevista la possibilità di utilizzare telecamere c.d. "indossabili": telecamere di dimensioni ridotte (es. telecamere di marca "GoPro" che possono essere indossate dagli agenti di Polizia Locale in servizio sul territorio, per documentare varie tipologie di reati ed illeciti.

L'utilizzo di telecamere indossabili è disciplinato come di seguito riportato.

26.1 - Designazione dei soggetti autorizzati ad utilizzare le telecamere indossabili

Il personale di Polizia Locale autorizzato ad utilizzare le telecamere indossabili deve essere individuato nominativamente per iscritto con atto a firma congiunta da parte del Sindaco e del Responsabile del servizio di Polizia Locale, mediante atto di nomina con il quale il soggetto autorizzato viene designato in qualità di incaricato del trattamento dei dati (o di "soggetto designato" ai sensi dell'art. 29 del GDPR).

26.2 - Tempi di conservazione delle immagini

Le immagini registrate mediante le telecamere indossabili devono essere conservate per un periodo di sette giorni solari. Qualora non siano disponibili meccanismi automatici mediante i quali le immagini sono automaticamente cancellate trascorsi sette giorni solari dalla data di acquisizione, devono essere previsti meccanismi manuali di cancellazione delle immagini e delle riprese filmiche.

26.3 - Utilizzi esplicitamente vietati

Le immagini e le riprese filmiche non potranno essere utilizzate per effettuare attività di controllo a distanza del personale, ne' per valutare le prestazioni e le performance dei lavoratori; inoltre, le immagini e le riprese filmiche acquisite mediante telecamere indossabili non possono essere utilizzate per irrogare sanzioni disciplinari.

Le telecamere indossabili non possono essere utilizzate all'interno dei mezzi di servizio in dotazione alla Polizia Locale e all'interno dei locali del Comune di Jesolo.

E' esplicitamente vietato qualsiasi tipo di diffusione delle immagini registrate, con particolare riferimento alla diffusione mediante pubblicazione su internet (es. pubblicazione su social network).

26.4 - Casi nei quali possono essere utilizzate le telecamere indossabili

Le telecamere indossabili possono essere utilizzate nelle situazioni nelle quali via sia un elevato e concreto rischio di resistenza agli agenti di Polizia Locale, risse, fuga dei trasgressori etc. In questa casistica rientrano senz'altro le attività di contrasto all'occupazione abusiva di suolo pubblico e le attività di sequestro o confisca di merci. Ulteriori casistiche nelle quali sia concesso l'utilizzo delle telecamere indossabili possono essere individuate con atto scritto da parte del Comandante.

26.5 - Luogo di custodia delle telecamere

Quando non utilizzate (es. alla fine del turno di pattuglia sul territorio), le telecamere devono essere custodite in sicurezza in un luogo o locale dotato di serratura, tenuto di norma chiuso a chiave.

L'accesso al suddetto luogo o locale deve essere controllato, e i soggetti autorizzati ad accedervi devono essere individuati nominativamente per iscritto. Deve essere adottata ogni ragionevole cautela per evitare il furto, il danneggiamento e la manomissione delle telecamere indossabili.

26.6 - Inventario delle telecamere indossabili

Deve essere tenuto e regolarmente aggiornato un inventario delle telecamere indossabili in dotazione al Comando di Polizia Locale del Comune di Jesolo. Detto inventario deve riportare come minimo le seguenti informazioni:

- marca e modello della telecamera indossabile
- capacità di memorizzazione
- risoluzione massima di acquisizione delle immagini e delle riprese filmiche
- nominativo del soggetto al quale la telecamera sia eventualmente stabilmente affidata.

26.7 - Scarico (estrazione) delle riprese filmiche rilevanti

Qualora durante le attività sul territorio le telecamere indossabili siano state utilizzate per documentare episodi rilevanti (es. resistenze agli agenti di Polizia Locale, risse, aggressioni etc.), all'atto del rientro presso il Comando di Polizia Locale, le sequenze filmiche devono essere scaricate in sicurezza su server all'interno di apposito spazio di memorizzazione organizzato come segue:

- deve essere creata una cartella denominata "*GOPRO*", seguita dalla data in cui le immagini sono state rilevate (es. "*GOPRO20140704*")
- all'interno della cartella i files o la struttura dati relativa all'estrazione devono denominati in modo significativo, cosicché sia possibile risalire all'evento (es. "RISSA-PIAZZA-MAZZINI").

26.8 - Obbligo di documentazione all'interno della relazione di servizio

Qualora alla fine del servizio si sia proceduto allo scarico (estrazione) delle immagini o delle riprese filmiche come previsto al punto precedente, il fatto deve essere documentato all'interno della relazione di servizio; in particolare nella relazione di servizio si dovrà riportare l'evento che è stato documentato mediante le riprese filmiche, il luogo nel quale si è verificato l'evento, nonché ogni informazione utile per poter identificare le riprese filmiche estratte (nome della cartella e nome dei files estratti).

Art. 27 – Utilizzo di sistemi a pilotaggio remoto ("Droni")

E' prevista la possibilità di utilizzare sistemi a pilotaggio remoto, detti anche "droni", per videosorvegliare aree altrimenti non coperte o scarsamente coperte dalla videosorveglianza mediante telecamere fisse o mobili.

L'utilizzo di droni è disciplinato come di seguito riportato.

27.1 - Designazione dei soggetti autorizzati ad utilizzare i droni

Il personale di Polizia Locale autorizzato ad utilizzare i droni deve essere individuato nominativamente per iscritto con atto a firma congiunta da parte del Sindaco e del Responsabile del servizio di Polizia Locale, mediante atto di nomina con il quale il soggetto autorizzato viene designato in qualità di incaricato del trattamento dei dati (o di "soggetto designato" ai sensi dell'art. 29 del GDPR).

27.2 - Tempi di conservazione delle immagini

Le immagini registrate mediante droni devono essere conservate per un periodo di sette giorni solari. Qualora non siano disponibili meccanismi automatici mediante i quali le immagini sono automaticamente cancellate trascorsi sette giorni solari dalla data di acquisizione, devono essere previsti meccanismi manuali di cancellazione delle immagini e delle riprese filmiche.

27.3 - Utilizzi esplicitamente vietati

I droni non possono essere utilizzati per videosorvegliare, nei limiti del possibile, in maniera sistematica o continuativa aree o pertinenze private, come ad esempio giardini, terrazze, attici etc., in quanto ciò costituirebbe, ai sensi dell'art. 615 bis del Codice Penale, reato di interferenze illecite nella vita privata. Parimenti i droni non possono essere utilizzati per videosorvegliare zone sensibili, come ad esempio aeroporti, caserme, installazioni militari etc.) o zone dove una eventuale caduta (ad esempio a causa dell'esaurimento dalla carica delle batterie) potrebbe provocare allarme, danni o disservizi (es. impianti chimici, raffinerie etc.).

27.4 - Dichiarazione di conformità al GDPR

I droni dovranno essere conformi alla disciplina rilevante in materia di protezione dei dati, con particolare riferimento al GDPR, al D.Lgs. 196/2003 così come modificato dal D.Lgs. 101/2018, ai Provvedimenti del Garante per la protezione dei dati personali; la succitata conformità dovrà essere dichiarata e certificata per iscritto da parte del fornitore degli apparati stessi.

27.4 - Privacy by design e privacy by default

I droni dovranno essere prodotti e configurati in conformità ai principi di privacy by design e privacy by default di cui all'art. 25 del GDPR; tale conformità dovrà essere dichiarata e certificata per iscritto da parte del fornitore degli apparati.

27.4 - Cifratura dei dati

Conformemente a quanto previsto dall'art. 32 comma 1 lettera a) del GDPR, i dati trattati mediante droni dovranno essere cifrati.

27.5 - Luogo di custodia dei droni

Quando non utilizzati (es. alla fine del turno di pattuglia sul territorio), I droni devono essere custoditi in sicurezza in un luogo o locale dotato di serratura, tenuto di norma chiuso a chiave.

L'accesso al suddetto luogo o locale deve essere controllato, e i soggetti autorizzati ad accedervi devono essere individuati nominativamente per iscritto. Deve essere adottata ogni ragionevole cautela per evitare il furto, il danneggiamento e la manomissione dei droni.

27.7 - Scarico (estrazione) delle riprese filmiche rilevanti

Qualora i droni siano stati utilizzate per documentare episodi rilevanti, all'atto del rientro presso il Comando di Polizia Locale, le sequenze filmiche devono essere scaricate in sicurezza su server all'interno di apposito spazio di memorizzazione organizzato come segue:

- deve essere creata una cartella denominata "*DRONE*", seguita dalla data in cui le immagini sono state rilevate (es. "*DRONE20101025*")
- all'interno della cartella i files o la struttura dati relativa all'estrazione devono denominati in modo significativo, cosicché sia possibile risalire all'evento (es. "ABBANDONO-RIFIUTI-PIAZZA MAZZINI").

27.8 - Obbligo di documentazione all'interno della relazione di servizio

Qualora alla fine del servizio si sia proceduto allo scarico (estrazione) delle immagini o delle riprese filmiche come previsto al punto precedente, il fatto deve essere documentato all'interno della relazione di servizio; in particolare nella relazione di servizio si dovrà riportare l'evento che è stato documentato mediante le riprese filmiche, il luogo nel quale si è verificato l'evento, nonché ogni

informazione utile per poter identificare le riprese filmiche estratte (nome della cartella e nome dei files estratti).

Art. 28 – Informativa

I cittadini devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa "minima". In luoghi diversi dalle aree esterne il modello va integrato con almeno un avviso circostanziato che riporti, oltre agli elementi dell'informativa minima", anche gli altri elementi previsti dall'art. 13 del GDPR.

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

E' necessario controllare periodicamente, con frequenza almeno mensile, che i cartelli siano presenti e ben leggibili, e non siano stati oggetto di atti vandalici o di eventi (es. crescita di rami o foglie, interposizione di altri elementi, etc.) che abbiano compromesso la piena leggibilità del testo e della rappresentazione iconica. In ogni caso, la leggibilità dovrà essere tempestivamente ripristinata e assicurata. Nella pagina seguente si riporta l'informativa che si dovrà affiggere bene in vista presso ciascuna telecamera.

Art. 29 – Riscontro all'interessato

In caso di esercizio da parte degli interessati dei diritti previsti dagli artt. Da 15 a 22 del GDPR, il riscontro all'interessato dovrà venire fornito a cura del Titolare o da Responsabile del trattamento dei dati appositamente designato dal Titolare, **entro 15 giorni lavorativi dalla data di ricezione della richiesta**. Le richieste di cancellazione o blocco dei dati dovranno essere soddisfatte esclusivamente nei casi in cui il trattamento sia avvenuto in violazione di legge, e comunque solo su autorizzazione scritta del Sindaco di Jesolo. Non potranno essere oggetto di cancellazione o modifica le immagini per le quali vi siano state richieste di estrazione o siano in corso indagini da parte degli organi di Polizia o da parte dell'Autorità Giudiziaria.

Art. 30 – 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 ad utilizzo non promiscuo e dedicato esclusivamente a "sala macchine" o "sala server", non agevolmente accessibile al pubblico e ai dipendenti (ad eccezione ovviamente dei dipendenti o collaboratori esplicitamente incaricati di operazioni di amministrazione e gestione di sistema);

- possibilità di regolamentare e di tenere traccia degli accessi al locale;
- locale di norma chiuso a chiave, con serratura e chiave funzionante;
- in caso vi siano finestre a piano terra, presenza di inferriate in ferro non dolce oppure presenza di vetri antisfondamento;
- 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;
- presenza di adeguato impianto di condizionamento, che assicuri un livello di umidità e temperatura all'interno del range di corretto funzionamento degli apparati.

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;
- presenza di sensori per la rilevazione del fumo e/o della temperatura;
- collegamento dei sensori e dell'allarme con centrale operativa di sicurezza oppure con le forze dell'ordine.

Art. 31 – Registrazione delle Operazioni effettuate

Ai sensi dell'art. 21 del D.Lgs. 51/2019, le operazioni di estrazione, modifica, consultazione, comunicazione, trasferimento, interconnessione e cancellazione di dati, dovranno essere sono registrate in appositi file di log, da conservare per la durata stabilita con il decreto di cui all'articolo 5, comma 2 del D.Lgs. 51/2018.

Le registrazioni delle operazioni di cui sopra debbono consentire di conoscere i motivi, la data e l'ora di tali operazioni e, se possibile, di identificare la persona che ha eseguito le operazioni e i destinatari.

Per poter soddisfare I requisiti di cui sopra, è necessario che ciascun operatore acceda al sistema con una propria user-id (e relativa password associata) personale, con profilo diverso da administrator.

Sono tassativamente vietate situazioni in cui i vari operatori accedono con la medesima user-id.

Le registrazioni sono usate ai soli fini della verifica della liceita' del trattamento, per finalita' di controllo interno, per garantire l'integrita' e la sicurezza dei dati personali e nell'ambito di procedimenti penali.

Su richiesta e fatto salvo quanto previsto dall'articolo 37, comma 3, il titolare del trattamento e il responsabile del trattamento mettono le registrazioni a disposizione del Garante.

Art. 32 – Sicurezza del Trattamento

Ai sensi ed in ottemperanza a quanto previsto dall'art. 25 del D.Lgs. 51/2018, dovranno essere messe in atto le seguenti misure di sicurezza:

1. Tenuto conto delle cognizioni tecniche disponibili, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalita' del trattamento, nonche' del grado di rischio per i diritti e le liberta' delle persone fisiche, devono essere messe in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio di violazione dei dati.

2. Per il trattamento automatizzato, previa valutazione dei rischi, devono essere adottate misure volte a:

a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);

b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);

c) impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);

e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

f) garantire la possibilita' di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);

g) garantire la possibilita' di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);

i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);

l) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilita'») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrita'»).

Art. 33 – Valutazione d'Impatto sulla Protezione dei Dati

Ai sensi dell'art. 23 del D.Lgs. 51/2019, il sistema di videosorveglianza potrà essere sottoposto a valutazione d'impatto sulla protezione dei dati, qualora il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

La valutazione d'impatto dovrà contenere come minimo una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le liberta' degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente regolamento.

Art. 34 - Effettuazione periodica di scansioni di vulnerabilità sulle piattaforme in cloud

Nel caso siano utilizzate piattaforme in cloud (ad esempio E-Surv), dovranno essere effettuate con frequenza mensile delle scansioni di vulnerabilità per individuare e documentare debolezze e configurazioni poco sicure, e per svolgere le attività di remediation.

Le scansioni di vulnerabilità verranno effettuate a cura del Responsabile della protezione dei dati con frequenza orientativamente mensile utilizzando piattaforme professionali di vulnerability assessment.

A fronte di richiesta da parte del Sindaco o del Responsabile del Servizio di Polizia Locale, potranno venire effettuate su una-tantum delle scansioni di vulnerabilità su altri oggetti esposti direttamente su internet, come ad esempio firewall, router etc

Art. 35 - Notificazione al Garante degli eventi di tipo "Violazione dei dati personali"

Nel caso si verifichi un qualsiasi tipo di violazione dei dati, o se ne abbia anche solamente il sospetto, ne deve essere data immediata comunicazione al Sindaco, al Responsabile del Servizio di Polizia Locale e al Responsabile della protezione dei dati, il quale si attiverà immediatamente per valutare se vi sia stata

effettivamente una violazione, la portata e le conseguenze, e valutare se sussistano i presupposti per effettuare la notificazione entro 72 ore all'autorità di controllo.

Art. 36 - Registro delle violazioni dei dati

Coerentemente con quanto previsto dall'art. 33 comma 5 del GDPR, deve essere in ogni caso tenuto un registro di tutte le violazioni di dati verificatesi, a prescindere dal fatto che siano state notificate all'autorità di controllo. Il suddetto registro deve contenere come minimo le seguenti informazioni:

- data della violazione
- descrizione delle circostanze e dell'evento
- tipologia e quantità di interessati impattati
- conseguenze della violazione
- data di comunicazione della violazione al Garante per la protezione dei dati (se la comunicazione è stata effettuata).

Art. 37 – 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;
- server e client protetti da password iniziale di accesso al sistema operativo e alle risorse di rete; possibilità da parte dell'utente finale di modificare autonomamente la propria password; possibilità da parte dell'amministratore di sistema di disabilitare la user-id senza cancellarla;
- server e client protetti da password iniziale di accesso al programma applicativo; possibilità da parte dell'utente finale di modificare autonomamente le propria password; possibilità di disabilitare (da parte dell'amministratore di sistema) le user-id senza cancellarla;
- 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.

I requisiti di cui sopra dovranno essere verificati con frequenza almeno semestrale mediante verifiche in loco dei locali, degli apparati e dei programmi, effettuando un'analisi dei rischi e individuando le azioni correttive da mettere in atto. Periodicamente si dovrà inoltre verificare che le misure pianificate siano state messe in atto, e il livello di efficacia delle misure stesse. Di tutto quanto appena elencato si dovrà redigere apposita relazione da discutere con il Comandante della Polizia Locale.

Art. 38 – Notificazione del trattamento al Garante per la protezione dei dati personali

Con l'entrata in vigore del D.Lgs. 101/2018, l'art. 37 del D.Lgs. 196/2003, che richiedeva per alcuni trattamenti l'obbligo di notifica del trattamento al Garante per la protezione dei dati personali, è stato abrogato.

Non è pertanto necessario effettuare alcuna notificazione al Garante per la protezione dei dati personali) dei trattamenti effettuati con il sistema di Videosorveglianza, con le fototrappole e con le telecamere indossabili.

Art. 39 – Cessazione del trattamento

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

Art. 40 – Danni cagionati per effetto del trattamento dei dati personali

La materia è disciplinata dall'art. 82 del GDPR.

Art. 41 – Comunicazione

La comunicazione di dati personali da parte del titolare ad altri soggetti pubblici è ammessa quando è prevista da norma di legge o di regolamento attuativo di norma di legge, oppure quando risulti comunque necessaria per lo svolgimento delle funzioni istituzionali.

La comunicazione di dati personali da parte del titolare a privati o ad enti pubblici economici è ammessa unicamente quando prevista da norma di legge o di regolamento.

Art. 42 – Modifiche e integrazioni regolamentari

Il presente regolamento dovrà essere adeguato per recepire eventuali modifiche alla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento alle disposizioni relative alla videosorveglianza.

Inoltre, il presente regolamento dovrà venire modificato nel caso dovessero mutare le finalità del sistema di videosorveglianza oppure introdotte significative novità di tipo tecnologico.

ALLEGATO 1

Comune di Jesolo

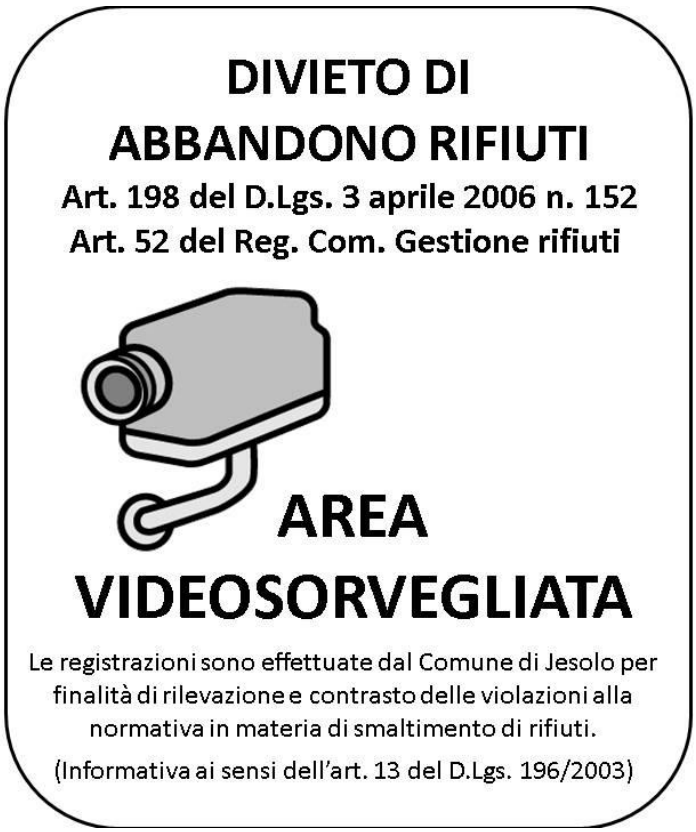
Provincia di Venezia

AREA VIDEOSORVEGLIATA

Le registrazioni sono effettuate dal Comune di Jesolo per le finalità di cui all'art. 5 del Regolamento di Videosorveglianza

(Informativa ai sensi dell'art. 13 del D.Lgs. 196/2003)

ALLEGATO 2



Documento informatico sottoscritto con firma elettronica ai sensi e con gli effetti di cui agli artt. 20 e 21 del d.lgs. 7 marzo 2005 n.82 e ss. mm.; sostituisce il documento cartaceo e la firma autografa.