
# COMUNE DI LEVERANO
# Provincia di Lecce

## REGOLAMENTO PER LA DISCIPLINA DEL TRATTAMENTO DEI DATI PERSONALI ED UTILIZZO DEGLI IMPIANTI DI VIDEOSORVEGLIANZA

Conforme al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016

APPROVATO CON DELIBERAZIONE DI C.C. N._____DEL_____

# Indice

# Art. 1 - Definizioni

Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione dell'impianto di videosorveglianza nel territorio urbano, gestito ed impiegato dagli agenti di polizia locale dipendenti del Comune di Leverano e collegato alla centrale operativa della stessa Polizia Locale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento. Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Presso la centrale operativa della Polizia Locale sono posizionati monitor per la visione in diretta delle immagini riprese dalle telecamere.

Per tutto quanto non è dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dal Codice in materia di protezione dei dati personali, per brevità nel seguito chiamato anche semplicemente "Codice", approvato con Decreto Legislativo 30 giugno 2003, n.196, come modificato dal D. lgs. 10 agosto 2018 n. 101 (e successive modifiche intervenute), dalla Deliberazione 8 aprile 2010 relativa al provvedimento del Garante in materia di videosorveglianza pubblicato in Gazzetta Ufficiale nr. 99 del 29/04/2010 e successive modifiche intervenute, dal 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, per brevità nel seguito chiamato anche semplicemente "Regolamento UE" e/o "RGDP".

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento. Ai sensi dell'art. 4 del Regolamento UE si intende per:

a) ***"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) ***"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, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;

c) ***"Titolare"*** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

d) ***"Responsabile"*** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali;

Ai sensi dell'art. 2-ter del Codice si intende per:

**e)** ***"comunicazione"*** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

**f)** ***"diffusione"*** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

All'interno del presente documento si definisce inoltre:

**g)** ***"dati identificativi"*** i dati personali che permettono l'identificazione diretta dell'interessato;

**h)** ***"dati sensibili"*** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

**i)** ***"dati giudiziari"*** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a p) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

**j)** ***"incaricati"*** le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;

**k)** ***"interessato"*** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

**l)** ***"dato anonimo"*** il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

**m)** ***"blocco"*** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

**n)** ***"banca di dati"*** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, formatosi presso la sala di controllo, e trattato esclusivamente mediante riprese video che, in relazione ai luoghi di installazione delle videocamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;

**o)** ***"Garante"*** l'autorità di cui all'articolo 153 del Codice;

**p)** ***"misure minime"*** il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti;

**q)** ***"strumenti elettronici"*** gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

**r)** ***"autenticazione informatica"*** l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

**s)** ***"credenziali di autenticazione"*** i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

t) *"parola chiave"* componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

u) *"profilo autorizzazione"* l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

v) *"sistema autorizzazione"* l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

w) *"rischi"* Situazioni o comportamenti che possano generare un pericolo per i dati personali e/o sensibili. Per meglio valutare l'entità e le azioni da intraprendere il rischio prevede diversi livelli di soglia: basso, medio, grave o gravissimo;

## Art. 2 - Obiettivo del presente Regolamento

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

- alle prescrizioni del Codice;
- alle prescrizioni del Regolamento UE;
- 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.

## 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 Leverano

## Art. 4 - Identificazione del Titolare del trattamento dei dati

Il Titolare dei trattamenti di dati personali effettuati mediante i sistemi di videosorveglianza installati nel territorio del Comune di Leverano è il Comune di Leverano: pertanto, competono esclusivamente al Comune di Leverano 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 Leverano:

- 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 trattamento dei dati personali è effettuato a seguito dell'attivazione di un impianto di telecontrollo e di videosorveglianza.

Il sistema di videosorveglianza, in quanto sistema che comporta il trattamento di dati personali, può essere utilizzato esclusivamente per il perseguimento delle funzioni istituzionali del Titolare del trattamento dei dati, vale a dire del Comune di Leverano.

Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza attengono allo svolgimento delle funzioni istituzionali che il Comune di Leverano in conformità a quanto previsto dal:

- D. Lgs. 18 agosto 2000, n. 267 – TUEL;
- D.P.R. 24 luglio 1977, n. 616;
- D. Lgs. 31 marzo 1998, n. 112;
- Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale;
- Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica;
- Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
- Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;
- Circolari del Ministero dell'Interno n.558/A/421.2/70/456 in data 8 febbraio 2005, n. 558/A421.2/70/195860 in data 6 agosto 2010 e n. 558/SICPART/421.2/70/224632 in data 02.03.2012.

Nella richiamata cornice normativa e all'interno del nuovo sistema di lotta alla criminalità che attribuisce agli Enti locali un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica, gli impianti di video sorveglianza installati nel territorio del Comune di Leverano sono precipuamente rivolti a garantire la sicurezza urbana che, l'art. 1 del Decreto del Ministero dell'Interno del 5 agosto del 2008, testualmente definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."

Le finalità istituzionali che possono essere perseguite mediante l'utilizzo del suddetto impianto sono coerenti e compatibili con le funzioni istituzionali del Comune di Leverano.
In via esemplificativa e non esaustiva le finalità sono:

a) attivazione di uno strumento operativo a supporto delle attività di protezione civile sul territorio del Comune di Leverano;

b) individuazione, in tempo reale, di luoghi e situazioni di ingorgo e delle cause, per consentire il pronto intervento della Polizia Locale e degli altri soggetti di cui all'art. 12 del D.lgs. n. 285/92;

c) comunicazione agli utenti della strada delle vie di maggiore intensità di traffico segnalando eventuali percorsi alternativi e/o ogni altra notizia utile sulla viabilità;

d) rilevazione di dati anonimi per l'analisi dei flussi di traffico e per la predisposizione dei piani urbani del traffico;

e) vigilanza sui luoghi di pubblico transito, in particolare nelle vie, piazze ed aree di mercato, giardini e parchi pubblici, aree antistanti e/o conducenti a scuole di ogni ordine e grado, aree antistanti e/o conducenti a fermate di servizi di linea, ai fini dell'attività ausiliaria di Pubblica Sicurezza e quindi di Polizia di Prevenzione e di Polizia Giudiziaria;

f) prevenzione e rilevazione di reati;

g) prevenzione e rilevazione di atti vandalici;

h) tutela del patrimonio del Comune di Leverano, di beni e di persone;

i) rilevazione situazioni di pericolo per la sicurezza urbana, consentendo l'intervento degli operatori;

j) 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;

k) sicurezza degli operatori.

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

## *I. Premessa*

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

## *II. 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 Leverano;
- 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 dalla norma, in tema per esempio di sicurezza presso stadi e impianti sportivi.

## *III. 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 del Comune di Leverano, 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.

## *IV. 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".

## *V. Principio di finalità*

Gli scopi perseguiti devono essere determinati, espliciti e legittimi; sono pertanto esclusi utilizzi

indeterminati, occulti e non legittimi. In particolare il Titolare o il Responsabile potranno perseguire solo finalità di sua pertinenza.

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

È 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

È 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 - Istituti scolastici

Il sistema di videosorveglianza attivo presso istituti scolastici dovrà garantire il diritto dello studente alla riservatezza (art. 2, comma 2, D.P.R. n. 249/1998), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione.

In tale quadro, potrà risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti.

È vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.

Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio.

## Art. 9 - Deposito di rifiuti

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

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

## Art. 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.

Il mancato rispetto di quanto sopra prescritto nelle lettere da a) ad f) comporta l'applicazione della sanzione amministrativa stabilita secondo i criteri dell'art. 166 del Codice.

## Art. 11 - 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 Leverano, 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. 12 - Accordi con enti pubblici e privati

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

## Art. 13 - Tipi di trattamenti autorizzati

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

- installazione e attivazione di nuove telecamere;
- creazione e gestione di gruppi e profili di utenti;
- consultazione immagini live da telecamera;
- messa a fuoco e brandeggiamento della telecamera;
- impostazione di limiti al brandeggiamento delle telecamere
- impostazione di zone oscurate staticamente
- registrazione di immagini;
- cancellazione di immagini;
- predisposizione delle soglie temporali e degli eventi di cancellazione immagini;
- consultazione immagini registrate;
- estrazione (duplicazione) immagini registrate;
- definizione aree di motion-detection;
- definizione azioni da eseguire in concomitanza di eventi di motion-detection;
- accensione di sorgenti luminose o ad infrarosso;
- attivazione funzionalità di "speak-ip";
- rilevazione e inventario degli indirizzi ip presenti in rete;
- rilevazione e inventario dei mac address presenti in rete;
- installazione e configurazione di software applicativo;
- installazione e configurazione di software di base;
- installazione di "patch" e "hot fix";
- attivazione collegamenti da remoto;
- interventi generici di manutenzione e configurazione hardware e software;
- attivazione e configurazione di meccanismi di logging ("tracciatura");
- estrazione e apposizione di forma digitale qualificata a files di log;
- conservazione per almeno un anno in luogo sicuro di files di log.

## Art. 14 - 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 del trattamento dei dati;
- Responsabile esterno del trattamento dei dati: sono i soggetti (persone fisiche o giuridiche) esterni al Comune di Leverano ai quali sono affidati 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 Leverano, 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. 15 - Obblighi per il Titolare del trattamento - Notificazione

Il Comune di Leverano nella sua qualità di Titolare del trattamento dei dati personali, rientrante nel campo di applicazione del presente regolamento, adempie agli obblighi di notificazione preventiva al Garante per la protezione dei dati personali, qualora ne ricorrano i presupposti.

## Art. 16 – Responsabile del trattamento ed Incaricati al Trattamento

Il Responsabile del Servizio della Polizia Locale del Comune di Leverano, o altra persona nominata dal Sindaco, è designato quale Responsabile del trattamento dei dati personali rilevati. È consentito il ricorso alla delega scritta di funzioni da parte del designato, previa approvazione del Sindaco del Comune di Leverano.

Il Responsabile 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 procede al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui ai commi 1 e 2 e delle proprie istruzioni.

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

Il responsabile, designa e nomina i preposti in numero sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito degli operatori di Polizia Locale.

Gli incaricati al trattamento dei dati devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare o del Responsabile.

Il Responsabile custodisce le chiavi per l'accesso ai locali della centrale di controllo, le chiavi degli armadi per la conservazione delle videocassette/cd o altro supporto informatico, nonché le parole chiave per l'utilizzo dei sistemi.

Il Responsabile del trattamento è tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente Regolamento.

Il Responsabile 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.

Le competenze proprie del Responsabile del trattamento sono analiticamente disciplinate nel contratto ovvero nell'atto giuridico avente forma scritta, con il quale il Titolare provvede alla sua designazione. In particolare:

i. *il Responsabile del trattamento individuerà e nominerà con propri atti gli Incaricati del trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, GDPR; detti incaricati saranno opportunamente istruiti e formati da parte del Responsabile del trattamento con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;*

ii. *il Responsabile del trattamento provvede a rendere l'informativa "minima" agli interessati secondo quanto definito al precedente art. 6;*

iii. *il Responsabile del trattamento verifica e controlla che il trattamento dei dati effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui all'art. 5 del GDPR e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;*

iv. *il Responsabile del trattamento assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;*

v. *il Responsabile del trattamento, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del GDPR;*

vi. *il Responsabile del trattamento assiste il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del GDPR;*

vii. *il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32, GDPR, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;*

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

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

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

xi. *il Responsabile del trattamento assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del GDPR e del precedente art. 7 del presente Regolamento e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del GDPR;*

xii. *il Responsabile del trattamento affianca il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del GDPR, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;*

xiii. *il Responsabile del trattamento garantisce che il Responsabile della Protezione dei Dati designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;*

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

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

xvi. *il Responsabile del trattamento assicura che gli incaricati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;*

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

xviii. *il Responsabile del trattamento vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.*

xix. *Il Responsabile interno del trattamento è autorizzato a ricorrere a Responsabili esterni del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato, in tutti i casi in cui egli, per la gestione/assistenza del sistema di videosorveglianza, faccia ricorso a soggetti esterni ai quali affidare incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente. In questi casi, il Responsabile interno del trattamento procederà a disciplinare i trattamenti da parte del responsabile esterno mediante contratto ovvero altro atto giuridico che vincoli il Responsabile esterno del trattamento al Titolare del trattamento ai sensi dell'art. 28, GDPR.*

Il Responsabile del trattamento dei dati procede ad individuare con proprio atto, le persone fisiche incaricate del trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni.

L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato. In ogni caso, prima dell'utilizzo degli impianti, gli incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.

Gli Incaricati procedono al trattamento attenendosi alle istruzioni impartite dal Responsabile il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari. In particolare, gli incaricati devono:

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

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

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

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

v. *evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile del trattamento dei dati;*

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

vii. *conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;*

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

Tra i soggetti designati quali incaricati verranno individuati, con l'atto di nomina, le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti magnetici.

Gli Incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del Responsabile.

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

## Art. 17 – Accesso ai dati da parte delle forze dell'ordine e dell'Autorità Giudiziaria

La comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico può 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 o dal Responsabile del Trattamento.

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 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. 18 – Accesso telematico da parte del Sindaco e dei Carabinieri e Polizia di Stato

È esplicitamente previsto che il Sindaco del Comune di Leverano, quale ufficiale di governo ai sensi dell'articolo 54 del D.lgs. n. 267 del 2000, sovrintendendo alla vigilanza su tutto quanto possa interessare la sicurezza e l'ordine pubblico del territorio comunale, disponga dell'accesso remoto in via telematica al sistema di Videosorveglianza, sia per assicurare la cooperazione della polizia locale con le Forze di polizia locale con le Forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'Interno, Autorità nazionale di Pubblica Sicurezza, sia per accelerare i tempi di indagine e per sgravare il personale di Polizia Locale del Comune di Leverano.

E' altresì 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 Leverano.

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. 19 - 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, 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 dei profili di accesso, dovrà essere effettuata dal Responsabile o dal Titolare del trattamento dei dati con frequenza almeno annuale.

## Art. 20 - Designazione degli incaricati del trattamento dei dati

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.

## Art. 21 - Modalità di raccolta dei dati personali

1) I dati personali oggetto di trattamento sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per le finalità di cui al precedente art. 3 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi, esatti e, se necessario, aggiornati;
   c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   d) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal successivo articolo 22;
   e) trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, di cui al precedente Art. 5 - comma 2, lett. d), con modalità volta a salvaguardare l'anonimato ed in ogni caso successivamente alla fase della raccolta, atteso che le immagini registrate possono contenere dati di carattere personale.
2) I dati personali sono ripresi attraverso le telecamere dell'impianto di telecontrollo e di videosorveglianza, installate in corrispondenza d'intersezioni, piazze, parchi pubblici e immobili, del territorio urbano, in conformità all'elenco dei siti di ripresa individuati dal Titolare del trattamento.
3) Le telecamere di cui al precedente comma 2 consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario. Inoltre alcune delle telecamere possono essere dotate di brandeggio, di zoom ottico e digitale, di infrarosso e collegate ad un centro di gestione ed archiviazione di tipo digitale.

Il Titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti

somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato.

I segnali video delle unità di ripresa saranno raccolti da una stazione di monitoraggio e controllo presso le sale controllo degli uffici di Polizia Locale. In questa sede le immagini saranno visualizzate su monitor e registrate su un supporto digitale. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, quando la sala di controllo non è presidiata.

## Art. 22 - Tempi di conservazione delle immagini

Le attività di videosorveglianza sono finalizzate alla tutela della sicurezza urbana e, alla luce delle recenti disposizioni normative, 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, il termine massimo di durata della conservazione dei dati è limitato ai **sette giorni successivi alla rilevazione** delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione.

In tutti i casi in cui si voglia procedere ad un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante, e comunque essere ipotizzata dal Titolare come eccezionale nel rispetto del principio di proporzionalità.

La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.

La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

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

In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal Titolare.

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". È inoltre prevista la possibilità che i tempi di memorizzazione delle immagini possano essere modificati a seguito di variazioni nelle finalità, di mutate esigenze, oppure di motivata richiesta proveniente da altri soggetti pubblici.

## Art. 23 - Criteri e modalità di estrazione delle immagini

L'estrazione di immagini o di intere riprese, mediante duplicazione e senza che vi sia cancellazione delle immagini registrate, potrà avvenire solo in presenza di autorizzazione scritta da parte del Sindaco del Comune di Leverano o del Responsabile di Polizia Locale / Comandante di Polizia locale nell'ambito della gestione in forma associata della funzione di polizia locale, rilasciata a fronte di richiesta scritta e motivata.

All'atto della consegna al soggetto richiedente del supporto di memorizzazione contenente le immagini estratte, l'operatore o chi materialmente consegnerà il suddetto supporto, dovrà far firmare e trattenere apposito documento che attesti la consegna e la ricevuta delle immagini estratte; detto documento dovrà fare riferimento alla richiesta originaria di estrazione.

Si dovrà inoltre compilare apposito registro dove si terrà traccia di:

- Soggetto che ha richiesto l'estrazione
- Generalità del soggetto che ha materialmente ritirato con mani proprie il supporto di memorizzazione
- Motivazione della richiesta di estrazione
- Numero di protocollo della richiesta di estrazione
- Numero di protocollo o riferimento univoco dell'autorizzazione all'estrazione
- Generalità del soggetto che ha materialmente effettuato il salvataggio delle immagini sul supporto di memorizzazione
- Giorno, data e ora di effettuazione dell'estrazione
- Numero di protocollo o identificazione univoca della ricevuta

Per le richieste di estrazione d'immagini, provenienti da cittadini o più in generale da interessati, esercitate ai sensi dell'art. 15 del Regolamento UE, potrà essere richiesto un contributo alle spese di ricerca ed estrazione delle immagini, in ogni caso non eccedente la somma di Euro 20,00 (per i dettagli si veda la Deliberazione n.14 del Garante, del 23 dicembre 2004, Gazzetta Ufficiale 8 marzo 2005 - n. 55).

## Art. 24 - Obblighi degli incaricati/operatori

L'utilizzo delle telecamere è consentito solo per la sorveglianza di quanto è ubicato oppure si svolge nelle aree pubbliche mentre esso non è ammesso nelle proprietà private.

L'utilizzo del brandeggio da parte degli operatori e degli incaricati al trattamento dovrà essere conforme ai limiti indicati nel documento di cui al punto 3 del precedente Art. 21.

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 o del Responsabile/Comandante la Polizia Locale 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/Responsabile della Polizia Locale.

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. 25 – Accertamenti d'illeciti ed indagini di Autorità Giudiziarie o di Polizia

Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, l'incaricato od il Responsabile della videosorveglianza provvederà a darne immediata comunicazione agli organi competenti.

In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa di cui ai precedenti Art. 21 e Art. 22, l'incaricato procederà alla registrazione delle stesse su supporti digitali.

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

L'apparato di videosorveglianza potrà essere utilizzato anche in relazione ad indagini di Autorità Giudiziaria, di organi di Polizia o di Polizia Locale.

Nel caso in cui gli organi della Polizia dello Stato o della Polizia Locale, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che sono contenute nelle riprese effettuate, possono farne richiesta scritta e motivata indirizzata al Responsabile della gestione e del trattamento dei dati.

## Art. 26 - Informazioni rese al momento della raccolta

Il Comune di Leverano in ottemperanza a quanto disposto dall'art. 12 del Regolamento UE e della deliberazione 8 aprile 2010 relativa al provvedimento del Garante in materia di videosorveglianza pubblicato in Gazzetta Ufficiale nr. 99 del 29/04/2010 e successive modifiche intervenute, si obbliga ad affiggere un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere, su cui è riportata la seguente dicitura: "Area Videosorvegliata – la registrazione viene effettuata dalla Polizia Locale del Comune di Leverano per fini riguardanti la Sicurezza Urbana - Art. 13 del Regolamento Generale in materia di Protezione dei Dati Personali (UE) 2016/679".


FIG. 1

Il Comune di Leverano nella persona del Responsabile, si obbliga a comunicare alla comunità cittadina l'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, l'eventuale incremento dimensionale dell'impianto e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo mediante appositi manifesti informativi e/o altri mezzi di diffusione locale e/o sul sito del Comune di Leverano.

Gli interessati dovranno essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).

A tal fine si ricorrerà all'utilizzo dello stesso modello semplificato di informativa "minima", indicante il Titolare del trattamento e la finalità perseguita, già individuato, ai sensi dell'art. 12, comma 7, del Regolamento UE, nel provvedimento del 2010 e riportato in fac-simile nell'allegato n. 1 al provvedimento dell'8 aprile 2010 (vedi FIG.1).

Il modello è ovviamente adattabile a varie circostanze.

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

In ogni caso il Titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Regolamento UE.

È necessario controllare periodicamente, con frequenza almeno trimestrale, 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.

## Art. 27 - 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. 28 - Installazione di telecamere mobili

È 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, abbandono rifiuti e superamento dei limiti di velocità etc.) telecamere mobili, senza ottenere l'autorizzazione preventiva da parte del Sindaco e della Giunta Comunale.

In ogni caso il Responsabile del Servizio di Polizia Locale dovrà avvertire il Sindaco quanto prima, comunque entro e non oltre dodici ore.

Tali telecamere potranno memorizzare i dati in locale, su apposita scheda SD installata a bordo della telecamera. A seconda delle finalità perseguite, potrà essere possibile non segnalare la presenza di telecamere mediante cartelli informativi.

Le telecamere mobili avranno la seguente tipologia: Telecamere Foto trappola, Bodycam, Scout Speed, mobilecam.

## Art. 29 - Riscontro all'interessato

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

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

b) di essere informato sugli estremi identificativi del Titolare e del Responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;

c) di ottenere, a cura del Responsabile, senza ritardo e comunque non oltre 15 giorni lavorativi dalla data di ricezione della richiesta, ovvero di 30 giorni lavorativi, previa comunicazione all'interessato, se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo:

   1) *la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento; la richiesta non può essere inoltrata dallo stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi;*

   2) *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;*

   3) *di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.*

Per ciascuna delle richieste di cui al comma 1, lett. c), n. 1), può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, definiti con atto formale dalla Giunta comunale secondo le modalità previste dalla normativa vigente.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

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

Le istanze di cui al presente articolo possono essere trasmesse al Titolare o al Responsabile anche mediante lettera raccomandata, telefax o posta elettronica o comunicata oralmente, che dovrà provvedere in merito entro e non oltre 15 giorni dalla data di ricezione della richiesta, ovvero di 30 giorni, previa comunicazione all'interessato, se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo.

Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (art. 15 del Regolamento UE).

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti

dal Regolamento UE.

In riferimento alle immagini registrate, non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo, viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.

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 del Comune di Leverano. 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 - Sistemi integrati di videosorveglianza

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

a) gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi Titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli Titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

b) collegamento telematico di diversi Titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; tale soggetto terzo, designato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE da parte di ogni singolo Titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun Titolare;

c) sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo Titolare, si può anche attivare un collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia. L'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il Titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia - individuato, ai sensi dell'art. 12, comma 7, del Regolamento UE, nel provvedimento del 2010 e riportato in fac-simile nell'allegato
n. 2 al citato provvedimento del Garante. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati.

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate nel precedente punto 3.3.1 del citato provvedimento del Garante, quali:

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

2) separazione logica delle immagini registrate dai diversi Titolari.

Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del

trattamento o agli effetti che possono determinare, il Titolare del trattamento è tenuto a richiedere una verifica preliminare al Garante.

## Art. 31 - Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e, in particolare, da enti territoriali

Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.

È stato individuato al punto 4.6 del citato provvedimento del 2010 del Garante un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale.

In particolare:

a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;

b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.

Il Titolare del trattamento è tenuto a richiedere una verifica preliminare al Garante fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già il punto 3.2.1 del citato provvedimento del Garante la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

## Art. 32 - Sicurezza dei dati

I dati personali oggetto di trattamento sono custoditi ai sensi e per gli effetti del precedente Art. 21 e Art. 22.

Alla sala controllo degli uffici della Polizia Locale presso il Comune di Leverano, dove sono custoditi i supporti di archiviazione digitali (server, videoregistratori, ecc.), può accedere, oltre il Sindaco o suo delegato, solo ed esclusivamente il personale in servizio della Polizia Locale, debitamente istruito sull'utilizzo dell'impianto e debitamente incaricato ed autorizzato per iscritto dal Responsabile individuato o suo delegato, nella loro qualità di Responsabile del trattamento dei dati personali ad effettuare le operazioni del trattamento dei dati.

Gli apparati di registrazione dell'impianto (NVR/DVR) sono ubicate presso la casa municipale del Comune di Leverano e non sono accessibili al pubblico.

I dati raccolti mediante sistemi di videosorveglianza dovranno essere protetti con idonee e

preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 32 e ss. del Regolamento UE).

Dovranno quindi essere adottate specifiche misure tecniche ed organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal Titolare medesimo, nel caso in cui questo sia persona fisica).

Le misure minime di sicurezza dovranno rispettare i seguenti principi:

a) *in presenza di differenti competenze specificatamente attribuite ai singoli operatori, devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati/incaricati o, eventualmente, Responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;*

b) *laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;*

c) *per quanto riguarda il periodo di conservazione delle immagini, devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;*

d) *nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni potranno accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;*

e) *qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale;*

f) *la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs).*

A norma delle disposizioni emanate dal Garante, si stabilisce che il Titolare o il Responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Si dovrà trattare di un numero delimitato di soggetti, specie quando il Titolare si avvale di collaboratori esterni, individuando altresì diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

Viene stabilito che, in presenza di differenti competenze specificatamente attribuite ai singoli operatori, devono essere configurati diversi livelli di visibilità e trattamento delle immagini.

Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati/incaricati o, eventualmente, Responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.

## Art. 33 - Luogo e modalità di memorizzazione delle immagini

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

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

## Art. 34 - 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:

- 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 sistemi in gradi di garantire 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. 35 - Iniziale deroga ai requisiti minimi sul luogo di collocazione del server

È comunque previsto dal presente regolamento che, a causa di vincoli e problematiche di varia natura, sia possibile collocare il server in un luogo che non soddisfi, soprattutto in una fase iniziale, tutti i requisiti elencati nel precedente articolo. In tal caso sarà sufficiente verificare e

assicurare che il server, e più in generale gli apparati coinvolti, non siano a rischio palese di asportazione, danneggiamento o manomissione. Ad esempio, potrà essere giudicata come temporaneamente accettabile una situazione in cui il server non sia collocato in un locale ad utilizzo dedicato, ma sia collocato un ufficio dove il personale presente negli orari d'ufficio possa assicurare a vista un adeguato presidio e controllo. Negli orari di chiusura ufficio o in caso di assenza di personale, potrà essere ritenuta sufficiente la presenza di una porta che sia però dotata di serratura e chiave funzionante, e possa essere tenuta chiusa in caso di assenza di personale.

## Art. 36 - 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 e s.m.i, relativo al controllo dell'operato degli amministratori di sistema, il presente Regolamento prevede quanto segue:

- a livello di software di videosorveglianza, deve essere attivato 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. 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; non sono consentiti sistemi operativi obsoleti o poco sicuri come ad esempio Windows 95 oppure Windows 98;
- 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 ed 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.

## Art. 38 – 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. 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 - Limiti alla utilizzabilità dei dati personali

La materia è disciplinata dall'art. 18 del Regolamento UE.

## Art. 41 - Comunicazione

La comunicazione di dati personali da parte del Titolare ad altri soggetti pubblici, esclusi gli enti pubblici economici, 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 e può essere iniziata se è decorso il termine di cui all'art. 2-ter, comma 2 del Codice.

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.

Non si considera comunicazione, ai sensi e per gli effetti del precedente paragrafo, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal Titolare o dal Responsabile e che operano sotto la loro diretta autorità.

## Art. 42 - Tutela amministrativa e giurisdizionale

Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dalla Parte III del Codice.

In sede amministrativa, il Responsabile del procedimento, ai sensi e per gli effetti degli artt. 4 e 6 della Legge 7 agosto 1990, n. 241 e successive modifiche intervenute, è il Responsabile del trattamento dei dati personali, così come individuato dal precedente Art. 16.

## Art. 43 - Modifiche e integrazioni regolamentari

Il presente regolamento dovrà essere adeguato nel caso in cui siano emanate eventuali modifiche alla disciplina relativa alla privacy e sicurezza dei dati, con particolare riferimento alle disposizioni e ai provvedimenti emanati dal Garante per la protezione dei dati personali.

Inoltre, il presente regolamento dovrà essere modificato nel caso dovessero mutare le finalità del sistema di videosorveglianza da parte del Consiglio comunale del Comune di Leverano.

## Art. 44 - Notificazione al Garante per la protezione dei dati personali

Stanti le finalità individuate all'Art. 5, non è necessario che i trattamenti di dati disciplinati nel presente regolamento siano notificati al Garante per la protezione dei dati personali, in quanto sono previsti all'interno del Provvedimento del 31 marzo 2004, pubblicato in G.U. n. 81 del 6 aprile 2004, avente ad oggetto i trattamenti sottratti all'obbligo di notificazione. Tuttavia, al Titolare viene data la facoltà in qualsiasi caso di effettuare la notifica (che comporterà però il pagamento di Euro 150,00 per diritti di segreteria), soprattutto laddove dovessero mutare in futuro alcuni elementi significativi.

## Art. 45 – Verifica preliminare da parte del Garante per la protezione dei dati personali

Al momento attuale non è necessaria la verifica preliminare da parte del Garante per le protezione dei dati personali, in quanto la suddetta verifica preliminare è necessaria solo ed esclusivamente nei casi indicati puntualmente all'interno del provvedimento del 8 aprile 2010 del Garante per le protezione dei dati personali.

## Art. 46 - Autorizzazione da parte del Garante per la protezione dei dati personali

Al momento attuale non è necessaria l'autorizzazione da parte del Garante per la protezione dei dati personali, in quanto tale autorizzazione è necessaria solo nel caso di trattamento di dati sensibili e giudiziari (es. riprese di persone malate o di detenuti).

## Art. 47 - Norme finali

Per quanto non disciplinato dal presente regolamento, si rinvia al Codice in materia di protezione dei dati personali, e al provvedimento generale sulla videosorveglianza emesso dal Garante per la protezione dei dati personali in data 8 aprile 2010.

## Art. 48 - Pubblicità e conoscibilità del regolamento

Il regime di eventuale pubblicità e conoscibilità del presente regolamento è disciplinato dallo Statuto del Comune di Leverano e dalla disciplina rilevante in materia di accesso agli atti e documenti amministrativi vigente nel Comune di Leverano.

## Art. 49 - Disposizione generale

Copia del presente Regolamento è depositato presso gli uffici di Polizia Locale del Comune di Leverano, a disposizione del Garante per la Protezione dei Dati Personali.