

REGOLAMENTO SULL'UTILIZZO DEGLI IMPIANTI DI VIDEOSORVEGLIANZA E SUL RELATIVO TRATTAMENTO DEI DATI

Approvato con Deliberazione dell'Assemblea n. ____ del ____/____/____

Sommario

CAPO I – DISPOSIZIONI GENERALI	4
Art. 1 - Oggetto del Regolamento	4
Art. 2 - Riferimenti normativi	4
Art. 3 – Principi.....	5
Art. 4 – Definizioni	7
Art. 5 – Finalità del Regolamento	8
Art. 6 – Caratteristiche tecniche dell’impianto e diretta visione delle immagini	9
Art. 7 – Telecamere mobili.....	9
Art. 8 – Telecamere modulari.....	10
Art. 9 - Trattamento di dati da parte di soggetti esterni.....	10
Art. 10 – Modalità di trattamento dei dati personali	10
CAPO II - OBBLIGHI DEL TITOLARE DEL TRATTAMENTO	10
Art. 11 – Titolarità del trattamento dei dati personali nei sistemi di videosorveglianza	10
Art. 12 – Valutazione d’impatto sulla protezione dei dati personali	11
Art. 13 – Responsabile del servizio ed Amministratore di sistema.....	11
Art. 14 - Responsabile della protezione dei dati.....	11
Art. 15 – Personale autorizzato al trattamento e persone autorizzate ad accedere ai dati	11
Art. 16 - Persone autorizzate ad accedere alle apparecchiature installate sul territorio	12
Art. 17 - Nomina a responsabile ex art. 28 Reg. Eu. 2016/679 per interventi tecnici sul sistema di videosorveglianza.....	12
CAPO III – TRATTAMENTO DEI DATI PERSONALI	13
Art. 18 – Modalità di raccolta e requisiti dei dati personali	13
Art. 19 – Prescrizioni da adottare per i dati trattati	14
Art. 20 – Informazioni rese al momento della raccolta dati	14
Art. 21 – Diritti dell’interessato	15
Art. 22 – Sicurezza dei dati	16
Art. 23 – Conclusione del trattamento dei dati.....	16
Art. 24 – Limitazioni ai diritti dell’interessato.....	17
Art. 25 – Diritto al risarcimento	17
Art. 26 – Comunicazioni	17
Art. 27 – Accertamento di illeciti ed indagini dell’ Autorità Giudiziaria o delle Forze di Polizia.....	17
CAPO IV – DISPOSIZIONI ATTUATIVE E FINALI	18
Art. 28 – Norme attuative.....	18
Art. 29 – Tutela amministrativa e giurisdizionale.....	18

Art. 30 – Impianti gestiti in contitolarità.....	18
Art. 31 - Tutela dei dati personali.....	18
Art. 32 - Pubblicità del regolamento	19
Art. 33 – Sopravvenienza di nuove disposizioni normative.....	19
Art. 34 - Entrata in vigore e successive modifiche del regolamento.....	19

CAPO I – DISPOSIZIONI GENERALI

Art. 1 - Oggetto del Regolamento

1. Il presente regolamento disciplina il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e i sistemi di lettura targhe attivati nel territorio del Nuovo Circondario Imolese, illustrando le misure adottate per conformare il trattamento in questione ai requisiti del Regolamento (UE) 2016/679, a quelli della Direttiva (UE) 2016/680, nonché le normative nazionali che li applicano (D. Lgs. 196/2003, come novellato dal D. Lgs. 101/2018).

2. L'installazione e l'attivazione del sistema di videosorveglianza non devono essere sottoposte all'esame preventivo del Garante, ma è sufficiente che il trattamento dei dati personali, effettuato tramite tale tipo di impianto per lo svolgimento dei propri compiti istituzionali, avvenga previa informativa alle persone che stanno per accedere nell'area videosorvegliata, utilizzando a tale fine il modello semplificato predisposto in fac-simile dall'Autorità, e siano adottate idonee misure di sicurezza.

3. In particolare, il presente regolamento:

- a) individua gli impianti di videosorveglianza fissi, mobili e di lettura targhe di proprietà del Nuovo Circondario Imolese, o dei Comuni associati;
- b) definisce le caratteristiche e le modalità di utilizzo degli impianti di videosorveglianza;
- c) disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza.

4. Gli impianti di videosorveglianza attivati nel territorio del Nuovo Circondario Imolese:

- a) riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese e/o i veicoli;
- b) consentono unicamente riprese video-fotografiche;
- c) sono installati e gestiti dai soggetti individuati dal Nuovo Circondario Imolese.

5. La disciplina relativa al trattamento dati di cui al presente regolamento, si applica anche alle apparecchiature di rilevazione della targa dei veicoli in transito, apposte lungo i varchi di accesso perimetrali alla rete viaria, ai fini della sicurezza urbana, in quanto e nei limiti in cui consentono la ripresa delle immagini e la registrazione dei dati alfanumerici contenuti nelle targhe veicolari.

6. L'utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada, in considerazione della peculiarità dei fini istituzionali perseguiti, non è assoggettato alla disciplina di cui al presente regolamento, ma alle disposizioni dettate dal Garante della privacy nel decalogo dell'8 aprile 2010 al paragrafo 5.3 nonché dalla specifica normativa di settore.

Art. 2 - Riferimenti normativi

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

- Legge 7 marzo 1986, n. 65;
- Art. 54 del D. Lgs. 18 agosto 2000 n. 267 e successive modificazioni;
- **Decalogo del 29 novembre 2000** promosso dal Garante per la protezione di dati personali;
- **D.Lgs. 30 giugno 2003 n. 196**, "Codice in materia di protezione dei dati personali", come modificato e riformato dal D.lgs. n. 101/2018 recante le "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- Circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/N471;

- Provvedimento in materia di “Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali”. emanato dal Garante per la Protezione dei Dati Personali del 13 novembre 2007.
- Decreto del Ministero dell’interno datato 5 agosto 2008;
- **D.Lg. 23 febbraio 2009 n. 11, coordinato con Legge di conversione n. 38 del 23 aprile 2009** recante: "*Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*", ed in particolare dall'art. 6;
- "**Provvedimento in materia di videosorveglianza**" emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010
- **Regolamento UE n. 2016/679 – Regolamento generale sulla protezione dei dati personali** (di seguito anche RGPD) relativo “alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”;
- **Direttiva UE n. 2016/680** relativa “alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”;
- **Circolare n. 558/SICPART/422.2/47/316370** datato 8 giugno 2017 del Capo della Polizia, recante: “*Patti per l’attuazione della sicurezza urbana – Forza di Intervento Rapido*”;
- **Decreto del Presidente della Repubblica n. 15 del 15.01.2018**, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
- **D.Lgs. del 18 maggio 2018, n. 51**, recante: "Attuazione della direttiva (UE) 2016/680 del Parlamento e del consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, nonché alla libera circolazione dei tali dati e che abroga la decisione quadro 2008/977 GAI del Consiglio”;
- **D.Lgs. 10 agosto 2018 n. 101** recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento UE del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”;

Art. 3 – Principi

1. La videosorveglianza in ambito locale si fonda sui principi di cui all’art. 5 RGPD, ossia:

a) Principio di liceità

Il trattamento dei dati attraverso sistemi di videosorveglianza è lecito solo se è necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento in ossequio al disposto di cui all’art. 6, par. 1, lett. E), RGPD.

La videosorveglianza circondariale, pertanto, è consentita senza necessità di consenso da parte degli interessati.

La videosorveglianza deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi.

Vanno richiamate al riguardo le norme vigenti dell’ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell’immagine e degli altri luoghi cui è riconosciuta analoga tutela.

Appare inoltre evidente la necessità del rispetto delle norme del Codice Penale che vietano le intercettazioni di comunicazioni e conversazioni.

b) Principio di necessità

Poiché l'installazione di un sistema di videosorveglianza comporta in sostanza l'introduzione di un vincolo per il cittadino, ovvero di una limitazione e, comunque, di un condizionamento, va applicato il principio di necessità e, quindi, va escluso ogni uso superfluo ed evitati eccessi e ridondanze.

Ciascun sistema informativo e il relativo programma informatico vanno conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi. Il software va configurato anche in modo da cancellare periodicamente e automaticamente i dati registrati.

Se non è osservato il principio di necessità riguardante le installazioni delle apparecchiature, l'attività di videosorveglianza non è lecita.

c) Principio di proporzionalità

Nel commisurare la necessità di un sistema al grado di rischio presente in concreto, va evitata la rilevazione di dati in aree di attività che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza, come quando, ad esempio, le telecamere vengono installate solo per meri fini di apparenza e di prestigio.

Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti e/o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti, quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi.

Non risulta di regola giustificata un'attività di videosorveglianza rivolta non al controllo di eventi, situazioni e avvenimenti, ma a fini promozionali, turistici o pubblicitari, attraverso web cam o camera-on-line che rendano identificabili i soggetti ripresi.

Anche l'installazione meramente dimostrativa o artefatta di telecamere non funzionanti o per finzione, anche se non comporta trattamento di dati personali, può determinare forme di condizionamento nei movimenti e nei comportamenti delle persone in luoghi pubblici e privati e, pertanto, può essere legittimamente oggetto di contestazione.

La videosorveglianza è, quindi, lecita solo se è rispettato il cosiddetto principio di proporzionalità sia sotto il profilo della scelta operativa relativa alla tipologia di sistemi da installare, sia nelle varie fasi del trattamento.

Il principio di cui trattasi consente margini di libertà nella valutazione da parte del titolare del trattamento ma non comporta scelte del tutto discrezionali e insindacabili.

Si evita così un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli altri interessati.

In applicazione del predetto principio, devono essere delimitate rigorosamente:

- anche presso luoghi pubblici o aperti al pubblico, quando sia legittimo ed effettivo interesse per particolari finalità, la ripresa di luoghi privati o di accessi a edifici;
- l'utilizzazione di specifiche soluzioni quali il collegamento ad appositi "centri" cui inviare segnali di allarme sonoro o visivo, oppure l'adozione di interventi automatici per effetto di meccanismi o sistemi automatizzati d'allarme (chiusura accessi, afflusso di personale di vigilanza, etc.), tenendo anche conto che in caso di trattamenti volti a definire profili o personalità degli interessati, la normativa in materia prevede ulteriori garanzie;
- l'eventuale duplicazione delle immagini registrate;
- la creazione di una banca dati quando, per le finalità perseguite, è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini, senza registrazione (esempio per il monitoraggio del traffico o per il controllo del flusso ad uno sportello pubblico).

d) Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi. Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza.

I sistemi di videosorveglianza sono in realtà introdotti come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare 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 utili in caso di fatti illeciti.

In ogni caso, possono essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e 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, tanto più quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti. Le finalità così individuate devono essere correttamente riportate nell'informativa.

Art. 4 – Definizioni

1. Ai fini del presente regolamento, si adottano le seguenti definizioni:

- **"dato personale"**, ai sensi dell' art. 4 n.1 Reg. EU 2016/679, qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **"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;
- **"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;
- **"dati identificativi"**, i dati personali che permettono l'identificazione diretta dell'interessato;
- **"dati particolari"**, ai sensi dell'art. 9 Reg. EU 2016/679, i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché quelli genetici, dati biometrici (intesi a identificare in modo univoco una persona fisica), dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- **"titolare del trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **"responsabile del servizio"**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che sovrintende l'attività di videosorveglianza per conto del titolare del trattamento;
- **"responsabile della gestione dei dati"**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che sovrintende la gestione dell'infrastruttura di videosorveglianza

e tratta i dati per finalità di sviluppo, gestione, implementazione, manutenzione dei componenti hardware e software di tale infrastruttura;

- **"autorizzati al trattamento"** le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile del trattamento;
- **"interessato"**, la persona fisica cui si riferiscono i dati personali;
- **"terzo"**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **"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;
- **"comunicazione"**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal responsabile, dalle persone autorizzate, ai sensi dell'articolo 2- quaterdecies D.lgs. 196/2003 così come modificato dal D.lgs. 101/2018, 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;
- **"diffusione"**, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **"dato anonimizzato"**, il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- **"Polizia Locale"**, il Corpo di Polizia Locale del Nuovo Circondario Imolese, a cui i Comuni aderenti hanno conferito le funzioni di polizia amministrativa locale;
- **"impianto di videosorveglianza"**, l'insieme di componenti ed apparati, di natura hardware e software, che costituiscono un sistema di videosorveglianza urbana basato sulla ripresa di immagini e dati che provengano da apparati di ripresa installati su supporti fissi quali pali e/o sbracci.

Art. 5 – Finalità del Regolamento

1. La sicurezza rappresenta un bene primario verso cui la collettività manifesta un grande interesse e forti aspettative. Essa è declinabile sia nel concetto di ordine e sicurezza pubblica, sia in quello di sicurezza partecipata ed integrata, in cui ogni possibile strumento e ogni risorsa concorrono al mantenimento di una ordinata e civile convivenza e alla vivibilità e fruibilità degli spazi pubblici delle nostre città.

2. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'impianto di videosorveglianza nel territorio del Nuovo Circondario Imolese, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

3. Le finalità perseguite dal Nuovo Circondario Imolese sono conformi alle funzioni istituzionali demandate ad essi, in particolare dal D. Lgs. 18 agosto 2000 n. 267, dal D.P.R. 24 luglio 1977, n. 616, dalla legge 7 marzo 1986 n. 65, nonché dallo statuto e dai regolamenti dell'Ente.

4. Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali, in modo da escluderne il trattamento quando le finalità perseguite possono essere realizzate mediante l'utilizzo di dati anonimi, oppure in modo da poter trattare tali dati mediante modalità che permettano di identificare l'interessato solo in caso di necessità.

5. L'impianto di videosorveglianza, complessivamente inteso, è in particolare finalizzato a:

- a) tutela della sicurezza urbana;
- b) tutela dell'ordine e della sicurezza pubblica;
- c) prevenzione, accertamento e repressione di comportamenti illeciti;

- d) razionalizzazione e miglioramento dei servizi al pubblico;
- e) rilevazione, prevenzione e controllo delle infrazioni poste in essere dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla Legge;
- f) controllo di determinate aree ai fini della tutela ambientale;
- g) tutela di coloro che più necessitano di attenzione: bambini, giovani e anziani, portatori di handicap;
- h) monitoraggio del traffico e dell'accesso alle zone a traffico limitato;
- i) prevenzione, accertamento e repressione degli illeciti derivanti dal mancato rispetto delle normative concernenti il regolare smaltimento dei rifiuti;
- j) implementare il sistema di gestione centralizzata degli impianti semaforici;
- k) attivare uno strumento operativo di protezione civile sul territorio del Nuovo Circondario Imolese.
- l) tutela dei beni di proprietà o in gestione alle Amministrazioni comunali associate, nonché del patrimonio pubblico, per prevenire e reprimere atti di vandalismo o danneggiamento.

Art. 6 – Caratteristiche tecniche dell’impianto e diretta visione delle immagini

1. Il sistema di videosorveglianza è strutturato in 3 tipologie:

- Sistema telecamere lettura targhe;
- Sistema telecamere ambientali/contesto;
- Sistemi di telecamere mobili e telecamere modulari.

2. Per le prime due tipologie, il sistema si compone di una serie di telecamere collegate tra loro mediante rete di comunicazione riservata e comunicante esclusivamente con la Centrale Operativa ubicata presso il Comando di Polizia Locale.

3. Nel dettaglio, l’impianto risulta così strutturato:

- presso la Centrale Radio Operativa della Polizia Locale è possibile visualizzare, in tempo reale e contemporaneamente, le immagini di tutte le telecamere, ed interagire con i dispositivi di brandeggio e zoom;
- l’impianto provvede alla registrazione delle immagini, nelle modalità previste dai successivi articoli, rendendone possibile la visualizzazione successiva;
- le immagini video riprese dalle telecamere sono trasmesse alla Centrale Radio Operativa tramite un’infrastruttura dedicata.

Art. 7 – Telecamere mobili

1. Gli operatori di Polizia Locale possono utilizzare, per i servizi a maggior rischio operativo, delle telecamere portatili, da indossare sulla divisa esterna (cosiddette BODY CAM, ovvero telecamere a bordo uomo) e delle telecamere installate nei veicoli di servizio (cosiddette DASH CAM, ovvero telecamere a bordo dei veicoli di servizio), in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016 prot. N. 49612; il relativo trattamento dei dati è ricondotto nell’ambito dell’art. 53 del Codice Privacy e del D.Lgs 51/2018, trattandosi di *“dati personali direttamente correlati all’esercizio dei compiti di Polizia di prevenzione dei reati, di tutela all’ordine e della sicurezza pubblica, nonché di Polizia Giudiziaria”*.

2. Nell’ambito di alcuni servizi, la Polizia Locale può utilizzare telecamere mobili aviotrasportate, tramite droni pilotati da terra, per il rilevamento di incidenti stradali, per il controllo di aree difficilmente raggiungibili e per ogni altra attività rientrante nelle funzioni di Polizia Locale.

3. Il Comando di Polizia Locale curerà la predisposizione di uno specifico disciplinare tecnico interno per la corretta e legittima attivazione, gestione e custodia dei sopraccitati dispositivi, nonché della documentazione video realizzata.

4. Il trattamento dei dati personali raccolti con i predetti sistemi di ripresa devono rispettare i principi di cui all'art. 11 del Codice; in particolare, i dati personali oggetto del trattamento devono essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consente l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati.

Art. 8 – Telecamere modulari

1. Su tutto il territorio del Nuovo Circondario Imolese possono essere temporaneamente posizionate telecamere modulari (le cosiddette “foto trappole”).

2. Gli apparati di videosorveglianza modulare vengono posizionati secondo necessità, esclusivamente nei luoghi teatro di illeciti penali o amministrativi, quest'ultimi non altrimenti accertabili con le ordinarie metodologie di indagine.

3. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D.Lgs. 51/2018, che esimono il titolare dall'obbligo di informazione, si provvederà alla previa collocazione dell'adeguata cartellonistica per l'informativa agli utenti frequentatori di dette aree.

Art. 9 - Trattamento di dati da parte di soggetti esterni

1. I dati raccolti dal sistema di videosorveglianza, secondo le finalità e con le modalità di cui al presente regolamento, possono essere trattati:

- in caso di richiesta, dall'Autorità Giudiziaria;
- dalle forze di Polizia nazionali, tramite accordi diretti fra i singoli comandi;
- dai corpi e servizi di Polizia Locale, tramite accordi diretti fra i singoli comandi;
- dai corpi di Guardie giurate particolari, per l'accertamento di illeciti di specifica competenza, previa sottoscrizione di specifica convenzione;

Art. 10 – Modalità di trattamento dei dati personali

1. Il trattamento dei dati personali è effettuato a seguito dell'attivazione di telecamere con sistema LPR per il riconoscimento automatico delle targhe con OCR, telecamere di contesto con tecnologia IP, nonché degli strumenti elencati nel presente regolamento.

2. Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conformi alle funzioni istituzionali demandate all'Ente. La disponibilità tempestiva delle immagini presso il Servizio di Polizia Locale costituisce uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale sul territorio dell'Ente, in stretto raccordo con le forze di Polizia nazionali.

CAPO II - OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

Art. 11 – Titolarità del trattamento dei dati personali nei sistemi di videosorveglianza

1. Il titolare del trattamento è il Nuovo Circondario Imolese, nella persona del legale rappresentante *pro tempore*.

Art. 12 – Valutazione d’impatto sulla protezione dei dati personali

1. Il Nuovo Circondario Imolese, nella sua qualità di titolare del trattamento dei dati personali, adempie all’obbligo previsto dall’art. 35 Reg. Eu 2016/679 in tema di valutazione d’impatto sulla protezione dei dati personali.
2. Il titolare del trattamento consulta l’autorità di controllo qualora la valutazione d’impatto sulla protezione dei dati ai sensi del suindicato art. 35 presenti un rischio elevato per i diritti e le libertà delle persone fisiche, in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; osserva in ogni caso integralmente quanto previsto dall’art. 36 del medesimo regolamento comunitario.
3. Per i sistemi di lettura targhe, il Titolare rileva che tali sistemi si limitano ad una lettura delle targhe, senza altre associazioni con altri dati tali da provocare pregiudizio per gli interessati.

Art. 13 – Responsabile del servizio ed Amministratore di sistema

1. Il Nuovo Circondario Imolese, nella sua qualità di titolare del trattamento dei dati personali, designa con apposito atto il Responsabile del servizio di videosorveglianza e l’Amministratore di sistema. Tali soggetti devono rispettare pienamente quanto previsto in tema di trattamento dei dati personali dalle leggi vigenti e dalle disposizioni del presente regolamento.
2. Il Responsabile del servizio procede ad effettuare le attività di sua competenza attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 1 del presente articolo e delle proprie istruzioni.
3. I compiti affidati al Responsabile del servizio sono analiticamente specificati per iscritto, in sede di designazione.
4. Le persone autorizzate al trattamento dati devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni impartite dal titolare o dal responsabile del servizio.

Art. 14 - Responsabile della protezione dei dati

1. In relazione all’attività di videosorveglianza disciplinata dal presente regolamento, il Responsabile della Protezione dei dati è il soggetto individuato dall’Ente ai sensi degli art. 37 e ss. del Regolamento Europeo 2016/679, con i compiti previsti dalla medesima normativa.

Art. 15 – Personale autorizzato al trattamento e persone autorizzate ad accedere ai dati

1. L’accesso ai dati è consentito esclusivamente, oltre al Titolare o al suo delegato, al Responsabile del servizio, all’amministratore di sistema e alle persone autorizzate al trattamento degli stessi.
2. Il titolare del trattamento, su indicazione del responsabile del servizio, designa le persone autorizzate al trattamento in numero sufficiente a garantire la gestione del servizio di videosorveglianza.
3. Le persone autorizzate al trattamento devono essere nominate tra il personale che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
4. Eventuali accessi da parte di persone diverse da quelle indicate al precedente comma devono essere autorizzati, per iscritto, dal Responsabile del servizio. L’autorizzazione deve contenere il motivo

dell'accesso e se possibile il tempo necessario per lo svolgimento dell'attività autorizzata, nonché l'indicazione degli specifici compiti loro assegnati e puntuali prescrizioni per l'utilizzo dei sistemi.

5. Per le autorizzazioni di cui ai precedenti commi, il Titolare del trattamento può provvedere secondo quanto indicato dall'art. 2 quaterdecies del D.Lgs 196/2003 (così come modificato dal D.lgs. 101/2018) e dall'art. 29 – GDPR.

6. Prima dell'utilizzo degli impianti, le persone autorizzate al trattamento devono essere istruite al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.

7. Le persone autorizzate al trattamento di cui al presente regolamento sono tenute al puntuale rispetto delle istruzioni e alla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 16 - Persone autorizzate ad accedere alle apparecchiature installate sul territorio

1. L'accesso ai siti ove sono installate le apparecchiature di ripresa di videosorveglianza e di rilevamento targhe deve avvenire secondo le modalità indicate nel precedente art. 15.

2. Eventuali accessi ai siti ove sono installate le apparecchiature di ripresa di videosorveglianza e di rilevamento targhe da parte di persone diverse da quelle previste nel predetto art. 15 devono avvenire alla presenza dei soggetti già designati e/o autorizzati.

Art. 17 - Nomina a responsabile ex art. 28 Reg. Eu. 2016/679 per interventi tecnici sul sistema di videosorveglianza

1. Il titolare, qualora si rendesse necessario un intervento sul sistema informatico, può avvalersi di personale esterno, che può anche non coincidere con il soggetto incaricato della manutenzione dell'impianto.

2. Laddove ne sussistano i presupposti, tale soggetto sarà nominato dal titolare del trattamento, responsabile ex art. 28 Reg. EU 2016/679.

3. Il soggetto cui le attività sono affidate deve:

- essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione della normativa volta a proteggere i dati personali;
- ottemperare agli obblighi previsti dal D.lgs. 196/2003 (così come modificato dal D.lgs. 101/2018) e dal Reg. EU 2016/679 nonché dalla normativa relativa alla protezione dei dati personali.
- adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrarle nelle procedure già in essere;
- impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e allertare immediatamente il Titolare del trattamento (l'Ente) in caso di situazioni anomale o di emergenze;
- riconoscere il diritto del Titolare a verificare periodicamente l'applicazione delle norme di sicurezza adottate, il quale, in caso di interventi tecnici per la manutenzione del sistema informatico relativo alla videosorveglianza, richiede ed esige dall'installatore un documento dettagliato circa l'intervento effettuato e la sua conformità alle disposizioni previste dalla normativa relativa alla protezione dei dati personali.
- osservare quanto previsto dall'art. 28 del Reg. Eu. 2016/679.

CAPO III – TRATTAMENTO DEI DATI PERSONALI

Art. 18 – Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento sono:

- trattati su uno dei presupposti di liceità previsti dal Titolo I Capo II del D. Lgs. 196/2003, così come modificato dal D.lgs 101/2018, nonché di quanto previsto dall'art. 6 del Reg. EU 2016/679;
- raccolti, registrati in maniera esatta e tenuti aggiornati per le finalità di cui al precedente Capo I, art. 3 del presente regolamento e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi; i dati saranno raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- 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 dai successivi commi 6 e 7 del presente articolo;
- trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, 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;
- l'attività di videosorveglianza è effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione;
- il sistema informativo ed il relativo programma informatico sono conformati, già in origine, in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi.

2. I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza installate sul territorio del Nuovo Circondario Imolese, che potrà essere successivamente integrato con nuovi impianti, secondo gli sviluppi futuri del sistema, approvati dall'organo amministrativo competente.

3. L'individuazione dei luoghi da sottoporre a videosorveglianza, come anche previsto dal D.L. n. 11 del 2009 convertito in L. n. 38 del 2009 e nel rispetto delle finalità previste dal presente Regolamento, compete alla Giunta del Nuovo Circondario Imolese. In caso di eventuale incremento dimensionale dell'impianto, modifica o cessazione di punti di ripresa, si procederà con atto amministrativo del Responsabile del Servizio di cui all'art. 13, in attuazione di quanto previamente deliberato dalla summenzionata Giunta. L'elenco con l'indicazione dell'ubicazione delle apparecchiature viene mantenuto aggiornato con apposita deliberazione dalla medesima Giunta.

4. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo che la strumentazione informatica consente e comunque nel rispetto di quanto previsto dal presente regolamento e dalle norme applicabili e comunque solo in caso di effettiva necessità per il conseguimento delle finalità di cui al Capo I, art. 3, a seguito di regolare autorizzazione di volta in volta richiesta al Titolare del trattamento.

5. La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, anche di sanzioni amministrative.

6. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso dei sistemi di videosorveglianza descritti nel presente regolamento, tenuto conto delle finalità perseguite, è consentita per un massimo di trenta giorni successivi all'evento.

7. Il termine di cui al comma precedente può essere superato qualora i dati, le informazioni e le immagini raccolte siano oggetto di ulteriore attività di indagine da parte dell'Autorità giudiziaria, della Polizia Locale, o delle Forze di Polizia nazionali, finalizzate all'accertamento di illeciti, legati ad un evento già accaduto o ritenuto realmente incombente. In tali circostanze, gli elementi raccolti potranno essere ulteriormente trattati, sino al completamento delle relative procedure di accertamento, da parte degli organi preposti.

Art. 19 – Prescrizioni da adottare per i dati trattati

1. I monitor degli impianti di videosorveglianza ed i monitor dai quali è possibile visionare i dati acquisiti con i sistemi di videosorveglianza sono collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate.
2. L'accesso alle immagini da parte del responsabile del servizio e delle persone autorizzate al trattamento dei dati si limita alle attività oggetto della sorveglianza.
3. Nel caso le immagini siano conservate, i relativi supporti vengono custoditi, per l'intera durata della conservazione, in un armadio o simile struttura dotato di serratura, apribile solo dal Responsabile e dagli incaricati del trattamento dei dati.
4. La cancellazione delle immagini è garantita mediante gli strumenti e le procedure tecnologiche più avanzate.
5. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile, non permettendo il recupero dei dati in esso presenti.
6. L'accesso alle immagini ed ai dati personali è consentito:
 - al Responsabile del servizio, ed alle altre persone autorizzate, previste nel Capo II del presente Regolamento;
 - ai preposti alle indagini dell'Autorità Giudiziaria e di Polizia;
 - all'Amministratore di sistema dell'Ente ed alla ditta fornitrice dell'impianto nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione;
 - all'interessato debitamente autorizzato in quanto soggetto ripreso; nel caso di accesso ai dati da parte dell'interessato questi avrà visione solo delle immagini che lo riguardano direttamente e mediante apposita procedura, come previsto dall'allegato 1) del presente regolamento.
 - al rappresentante legale dell'Ente, presso cui è installato l'impianto di videosorveglianza che ha acquisito e conserva le immagini, in virtù dei poteri a lui conferiti in materia di sicurezza urbana ex art 54 D.lgs. 267/2000 (TUEL).
7. Fermo quanto previsto all'art. 11 Capo II del presente regolamento, tutti gli accessi alla visione vengono documentati in forma telematica idonea ad integrare ad ogni effetto il registro degli eventi e degli accessi, in modo che vengano riportati:
 - la data e l'ora d'accesso e di uscita;
 - l'identificazione del terzo autorizzato;
 - gli estremi e la motivazione dell'autorizzazione all'accesso;
 - la sottoscrizione del medesimo.
8. Non possono essere rilasciate copie delle immagini registrate concernenti altri soggetti diversi dall'interessato, salvi i casi particolarmente meritevoli di tutela.
9. La diffusione di immagini personali è consentita quando la persona interessata ha espresso il proprio consenso o è necessaria per la salvaguardia della vita o dell'incolumità fisica o è giustificata da necessità di giustizia o di polizia; essa è comunque effettuata con modalità tali da non recare pregiudizio alla dignità della persona.
10. Per la regolamentazione della comunicazione dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento, da parte del Titolare a favore di soggetti pubblici, esclusi gli enti pubblici economici, si veda il successivo art. 20.

Art. 20 – Informazioni rese al momento della raccolta dati

1. Il Nuovo Circondario Imolese, in ottemperanza a quanto disposto dall'art. 13 del Reg. EU 2016/679 espone un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le

telecamere, su cui è riportata idonea dicitura, secondo i provvedimenti emanati dalle competenti Autorità di sorveglianza.

- il supporto contenente le informazioni previste;
- deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile anche in orario notturno;
- deve inglobare un simbolo o una stilizzazione di esplicita ed immediata comprensione, eventualmente diversificati se le immagini sono solo visionate o anche registrate.

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

3. Il Nuovo Circondario Imolese provvederà a pubblicare sul proprio sito internet istituzionale un'informativa circostanziata contenente tutti gli elementi previsti dall'Art.13 del GDPR.

4. Come disposto dalla Circolare del Ministero dell'Interno – nr. 558/A/421.2/70/195969 del 6 agosto 2010, l'informativa di cui sopra non è obbligatoria nel caso di utilizzo di telecamere a scopo di tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

5. Il Nuovo Circondario Imolese, nella persona del legale rappresentante pro tempore, dovrà comunicare ai cittadini l'eventuale incremento dimensionale dell'impianto e l'eventuale successiva modifica o cessazione per qualsiasi causa del trattamento medesimo, ai sensi del successivo art. 20 del presente Capo, con un anticipo di giorni 15 (quindici), mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

Art. 21 – Diritti dell'interessato

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

- di chiedere in ogni momento all'intestato Ente la conferma dell'esistenza di trattamenti che possono riguardarlo nonché l'accesso ai propri dati personali, la rettifica degli stessi qualora non siano veritieri, nonché la loro cancellazione;
- di richiedere la limitazione del trattamento che lo riguarda, e può opporsi allo stesso laddove sia esercitato in modo illegittimo;
- l'apposita istanza relativa all'esercizio dei sopracitati diritti può essere presentata o al Titolare del trattamento o al Responsabile della protezione dei dati (R.P.D. / D.P.O) designato. Tale istanza deve essere corredata di ogni informazione e documentazione utile a dimostrare il legittimo interesse del richiedente.

2. 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.

3. 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.

4. La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti i dati attinenti alla persona richiedente e può comprendere eventuali dati riferiti a terzi, solo nei limiti previsti dalla Legge. A tal fine, la verifica dell'identità del richiedente deve avvenire mediante esibizione o allegazione di un documento di riconoscimento che evidenzia un'immagine riconoscibile dell'interessato.

5. Le istanze di cui al presente articolo possono essere trasmesse al titolare del trattamento o al responsabile della protezione dati (R.P.D / D.P.O.) secondo le modalità previste dall'art. 12, commi 3 e 4, di cui al Reg. EU 2016/679.

6. Nel caso in cui l'interessato venga autorizzato alla visione delle immagini, per l'esercizio dei diritti di cui al comma 1 del presente articolo, lo stesso potrà visionare le immagini secondo le modalità previste dal presente regolamento ed in ogni caso sotto la supervisione di personale autorizzato. La supervisione da parte di tali soggetti non è richiesta laddove l'interessato faccia accesso alle immagini accompagnato da personale di forza di polizia o esibendo un provvedimento dell'autorità giudiziaria che motivi l'accesso dell'interessato alle immagini. L'accesso sarà in ogni caso registrato ai sensi del Capo III, art. 19, comma 7 del presente regolamento.

7. Nel caso di esito negativo all'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.

Art. 22 – Sicurezza dei dati

1. I dati personali oggetto di trattamento sono custoditi secondo quanto previsto dal presente regolamento.

2. Presso la Centrale Radio Operativa della Polizia Locale, ove vengono visualizzati in tempo reale i dati raccolti, possono accedere solo ed esclusivamente le persone autorizzate.

3. Il sistema installato adotta le misure di sicurezza volte a ridurre i rischi di distruzione, perdita, anche accidentale delle informazioni, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta dei dati relativi alla videosorveglianza. Tali misure di sicurezza devono essere adottate anche in caso di aggiornamento del sistema.

4. Il titolare del trattamento adotta ogni accorgimento necessario per garantire la sicurezza fisica del dato, prevenire rischi dipendenti da comportamenti scorretti da parte dei soggetti autorizzati al trattamento dati, favorendo in loro una maggiore consapevolezza al riguardo.

5. I dispositivi di visualizzazione impiegati per la visione delle immagini, la consultazione ed interrogazione dei dati acquisiti dal sistema sono posizionati e gestiti dagli operatori in modo tale da non permetterne la visione, neanche occasionalmente, a persone estranee non autorizzate.

6. L'accesso alle immagini da parte dei soggetti autorizzati deve limitarsi alle attività oggetto di videosorveglianza. Eventuali altre informazioni di cui questi vengono a conoscenza, mentre osservano il comportamento di un soggetto ripreso, devono essere ignorate.

7. Nel caso in cui le immagini siano conservate per una specifica richiesta investigativa dell'autorità giudiziaria o di un organo di polizia giudiziaria, i relativi supporti di memorizzazione devono essere custoditi in maniera sicura e accessibili al solo Responsabile del servizio o alle persone autorizzate al trattamento.

8. La cancellazione dei dati deve avvenire con modalità sicure, tali da rendere irrecuperabile il dato ed impedirne la disponibilità ad alcun soggetto, anche mediante sovra-registrazione, così come indicato dal Garante per la Protezione dei Dati Personali con Provvedimento del 13 novembre 2007 e con provvedimento dello stesso Garante datato 08 aprile 2010, in tema di videosorveglianza.

Art. 23 – Conclusione del trattamento dei dati

1. In caso di conclusione, per qualsiasi causa, di un trattamento dati, gli elementi raccolti possono essere alternativamente distrutti, oppure conservati per finalità esclusivamente legate all'impianto di videosorveglianza.

Art. 24 – Limitazioni ai diritti dell’interessato

1. La materia è disciplinata dall'art. 2 undecies del Codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196, così come modificato dal D.lgs 101/2018 e dall’art. 18 del Reg. E.U 2016/679.

Art. 25 – Diritto al risarcimento

1. La materia è regolamentata dall'art. 152 del D.Lgs 196/2003, così come modificato dal D.lgs. 101/2018 e dall’art. 82 del Reg Eu 2016/679.

Art. 26 – Comunicazioni

1. La comunicazione dei dati personali da parte del Nuovo Circondario Imolese a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria ed esclusivamente effettuata per lo svolgimento delle funzioni istituzionali.

2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, 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.

3. È in ogni caso fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D.Lgs. 30/6/2003, n. 196, così come modificato dal D.lgs. 101/2018, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

4. Qualora sussistano i presupposti di cui all’art. 4 della Legge n. 300/1970, il sistema di videosorveglianza disciplinato dal presente regolamento viene posto in essere previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro.

Art. 27 – Accertamento di illeciti ed indagini dell’Autorità Giudiziaria o delle Forze di Polizia

1. 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, la persona autorizzata al trattamento di videosorveglianza provvederà a darne immediata comunicazione agli organi competenti.

2. In tali casi, anche in deroga alle prescrizioni di cui ai precedenti articoli, l’autorizzato al trattamento procederà agli ingrandimenti delle immagini strettamente necessari e non eccedenti allo specifico scopo perseguito ed alla registrazione delle stesse immagini su supporti magnetici.

3. Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli operatori di polizia e l’Autorità Giudiziaria.

4. Gli apparati potranno essere utilizzati anche in relazione ad indagini dell’Autorità Giudiziaria e degli operatori di Polizia Giudiziaria.

5. I trattamenti di dati personali dal Corpo di Polizia Locale effettuati per le finalità di polizia, quando direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati, sono disciplinati **dal Decreto del Presidente della**

Repubblica del 15 gennaio 2018, n. 15 "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia. (GU Serie Generale n.61 del 14-03-2018) e dal **D.Lgs del 18 maggio 2018, n. 51**, recante: "Attuazione della direttiva (UE) 2016/680 del Parlamento e del consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2018/977 GAI del Consiglio".

CAPO IV – DISPOSIZIONI ATTUATIVE E FINALI

Art. 28 – Norme attuative

1. Il Corpo di Polizia Locale, sentite anche le forze di Polizia nazionali, propone alla Giunta del Nuovo Circondario Imolese l'individuazione dei siti di ripresa e di ogni ulteriore disposizione ritenuta utile.
2. L'elenco dei punti di ripresa è indicato e viene mantenuto aggiornato con apposite deliberazioni della Giunta del Nuovo Circondario Imolese.
3. Il presente regolamento si colloca nella cornice normativa relativa allo svolgimento delle funzioni istituzionali dell'ente, ai sensi dell'articolo 2 ter, del D. Lgs 30 giugno 2003 n. 196, così come modificato dal D.Lgs 101/2018 e rappresenta il disciplinare d'uso dei servizi.
4. I contenuti del presente regolamento devono essere aggiornati nei casi di aggiornamento normativo in materia di trattamento dei dati personali.

Art. 29 – Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 140bis e seguenti del decreto legislativo 30 giugno 2003, n. 196, così come modificato dal D.lgs. 101/2018.
2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il Responsabile del servizio.

Art. 30 – Impianti gestiti in contitolarità

1. Qualora il Nuovo Circondario Imolese gestisca alcuni impianti di videosorveglianza in contitolarità con altri Titolari, le parti stipulano un accordo di contitolarità, ai sensi e per effetti degli artt. 26 e 79 del GDPR, dove vengono chiaramente definiti i rispettivi ruoli e le rispettive responsabilità, tra cui le modalità di esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni. L'accordo viene adeguatamente pubblicizzato, come previsto dalla normativa.

Art. 31 - Tutela dei dati personali

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

Art. 32 - Pubblicità del regolamento

1. Copia del presente regolamento, a norma dell'art. 22 della legge 7 agosto 1990, n. 241, è tenuta a disposizione del pubblico, perché ne possa prendere visione in qualsiasi momento.
2. Il presente regolamento verrà pubblicato all'Albo pretorio e sul sito internet istituzionale dell'Ente, nella sezione "amministrazione trasparente", ai sensi della vigente normativa in tema di pubblicazione degli atti amministrativi.

Art. 33 – Sopravvenienza di nuove disposizioni normative

1. Le disposizioni del presente regolamento si intendono modificate per effetto di sopravvenute norme vincolanti statali, regionali o comunitarie.
2. In tali casi, in attesa dell'approvazione delle modifiche, è applicata la normativa sovraordinata.
3. A seguito delle modifiche apportate, qualora ne sussistano i presupposti, il regolamento viene trasmesso al Garante per la protezione dei dati personali.

Art. 34 - Entrata in vigore e successive modifiche del regolamento

1. Il presente regolamento entra in vigore il giorno successivo alla pubblicazione della delibera di approvazione.