REGOLAMENTO PER LA DISCIPLINA DEL SISTEMA DI VIDEOSORVEGLIANZA NEL TERRITORIO DEL COMUNE DI INVERUNO (MI)

^ ^

approvato con Deliberazione di C. C. n. 12 del 24/04/2023

INDICE

CAPO I - PRINCIPI GENERALI

Articolo 1 - Oggetto e norme di riferimento

1. Il presente regolamento disciplina il trattamento dei dati personali, realizzato mediante l'impianto di videosorveglianza locale, attivato nel territorio urbano ed extra urbano del Comune di Inveruno (Mi) (d'ora in poi Comune per brevità).
2. Garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune, 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 immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. La videosorveglianza dà luogo pertanto a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.
4. Per tutto quanto non è dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dal GDPR – Reg. UE n. 679/2016, dal Decreto legislativo 10 agosto 2018, n. 101, dal D.P.R., 15/01/2018 n° 15, G.U. 14/03/2018, dalla direttiva 2016/280 (direttiva Polizia) attuata con D.Lgs. 18/05/2018 n. 51, dal Provvedimento Garante Privacy in materia di videosorveglianza 8 aprile 2010 e dalle linee guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video.
5. La Videosorveglianza in ambito Comunale si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5, RGDP e, in particolare:
Principio di liceità – Il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando 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, Paragrafo 1, lett. e), RGPD.
La videosorveglianza comunale pertanto è consentita senza necessità di consenso da parte degli interessati.
Principio di necessità – In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e 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. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.
Principio di proporzionalità – La raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro

installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.
Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere.
Principio di finalità – Ai sensi dell'art. 5, Paragrafo 1, lett. b), RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana.

Articolo 2 - Definizioni
1. Ai fini del presente regolamento si intende:
- per «dato personale», qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- per «trattamento», qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- per "banca dati", il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;
- per «profilazione», qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- per «pseudonimizzazione», il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- per «titolare del trattamento», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- per «responsabile del trattamento», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- per «incaricato del trattamento», la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del responsabile del trattamento;
- per "interessato", la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
- per «terzo», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- per «violazione dei dati personali», la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- per "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per "diffusione", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Articolo 3 - Finalità

1. Le finalità istituzionali del suddetto impianto sono del tutto conformi alle funzioni istituzionali demandate al Comune, in particolare dal D.lgs.18 agosto 2000 n. 267, dal D.P.R. 24 luglio 1977, n.616, dal D.Lgs.31 marzo 1998, dalla legge 7 marzo 1986 n. 65, sull'ordinamento della Polizia Locale, nonché dallo statuto e dai regolamenti del Comune. La disponibilità tempestiva di immagini presso il Comando della Polizia Locale costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dei compiti della Polizia Locale sul territorio comunale, in stretto raccordo con le forze dell'ordine.
2. Gli impianti di videosorveglianza, in sintesi, sono finalizzati:
a) a prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana", così individuata secondo il decreto legge 20 febbraio 2017, n. 14 recante "Disposizioni urgenti in materia di sicurezza delle città", pubblicato sulla Gazzetta Ufficiale n. 93 del 21 aprile 2017 insieme alla legge di conversione 18 aprile 2017, n. 48;
b) a tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e a prevenire eventuali atti di vandalismo o danneggiamento;
c) al controllo di determinate aree;
d) al monitoraggio del traffico;
e) a tutelare in tal modo coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un elevato grado di sicurezza nelle zone monitorate;
f) ad acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
g) per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;

h) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
i) verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.
3. Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.
4. Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.
Gli impianti di videosorveglianza non potranno essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica. L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.
5. L'uso dei dati personali nell'ambito definito dal presente Regolamento, non necessita del consenso degli interessati in quanto viene effettuato per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri e allo svolgimento di funzioni istituzionali di cui è investito il Comune.

CAPO II - OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

Articolo 4 Caratteristiche tecniche dell'impianto –Sale operative, di controllo e di registrazione

Il Sistema si compone di una rete di comunicazione dati e di telecamere collegate a:
- centrale operativa e di controllo costituita all'interno della sede del Comando di Polizia Locale del Comune di Inveruno attualmente ubicata presso la sede di via Sen. G. Marcora n. 38/40 a Inveruno (Mi) ove vengono registrate e visualizzate le immagini rilevate da tutte le postazioni;

Articolo 5 - Esercente le funzioni del trattamento dei dati personali

1. Il Responsabile del Servizio di Polizia Locale in servizio, o altra persona nominata dal Sindaco, domiciliati in ragione delle funzioni svolte in Inveruno presso il Comando della Polizia Locale, è individuato, previa nomina da effettuare con apposito decreto del Sindaco, quale esercente funzioni del trattamento dei dati personali rilevati, ai sensi dell'art. 2-quaterdecies del D.Lgs 196/2003. E' consentito il ricorso alla delega scritta di funzioni da parte del designato, previa autorizzazione del Sindaco.
2. L'esercente le funzioni del trattamento dei dati personali deve rispettare pienamente quanto previsto, in tema di trattamento dei dati personali, dalle leggi vigenti, ivi incluso il profilo della sicurezza e dalle disposizioni del presente regolamento.

3. L'esercente le funzioni del trattamento dei dati personali procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 1 e delle proprie istruzioni.
4. I compiti affidati all'esercente le funzioni del trattamento dei dati personali devono essere analiticamente specificati per iscritto, in sede di designazione prevedendo in particolare che:
-l'esercente le funzioni 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, RGPD; detti incaricati saranno opportunamente istruiti e formati da parte dell'esercente le funzioni 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;
-l'esercente le funzioni del trattamento provvede a rendere l'informativa "minima" agli interessati secondo quanto definito al precedente art. 6;
-l'esercente le funzioni 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 RGPD 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;
-l'esercente le funzioni del trattamento assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
-l'esercente le funzioni 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 RGPD;
-l'esercente le funzioni 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 RGPD;
-l'esercente le funzioni del trattamento assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32, RGPD, 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;
-l'esercente le funzioni 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;
-l'esercente le funzioni 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;

-l'esercente le funzioni del trattamento assiste il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;
-l'esercente le funzioni del trattamento assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD 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 RGPD;
-l'esercente le funzioni del trattamento affianca il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;
-l'esercente le funzioni 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;
-l'esercente le funzioni 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;
-l'esercente le funzioni 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;
-l'esercente le funzioni 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;
-l'esercente le funzioni 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;
-l'esercente le funzioni del trattamento vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.
L'esercente le funzioni 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, l'esercente le funzioni 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, RGPD
5. Gli incaricati del materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del titolare o dell'esercente le funzioni del trattamento dei dati personali

6. L'esercente le funzioni del trattamento dei dati personali 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.

Articolo 6 - Nomina degli incaricati alla gestione dell'impianto di videosorveglianza

1. L'esercente le funzioni del trattamento dei dati personali, designa e nomina gli incaricati in numero sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito degli operatori di Polizia Locale, così detti incaricati.
2. Gli incaricati andranno nominati tra gli Agenti in servizio presso il Servizio di Polizia Locale che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
3. La gestione dell'impianto di videosorveglianza è riservata agli organi di Polizia Locale, aventi qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del Codice di Procedura Penale.
4. Con l'atto di nomina, ai singoli incaricati saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.
7. Gli incaricati dei servizi di cui al presente regolamento vigilano sul puntuale rispetto delle istruzioni e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.
In particolare, gli incaricati devono:
-per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
-conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
-mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
-custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
-evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile del trattamento dei dati;
-mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
-conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
-fornire all'esercente le funzioni 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.
8. Nell'ambito degli incaricati, verranno designati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle password e delle chiavi di accesso alla sala operativa ed alle postazioni per l'estrapolazione delle immagini

9. 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.
10. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento, oltre che a partecipare a periodici corsi formativi.

Articolo 7 - Accesso ai sistemi e parole chiave
1. L'accesso ai sistemi è esclusivamente consentito all'esercente le funzioni del trattamento dei dati personali, agli incaricati come indicato nei punti precedenti.
2. Gli incaricati saranno dotati di propria password di accesso al sistema.
3. Il sistema dovrà essere fornito di "log" di accesso, che saranno conservati per la durata di anni uno.
L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 del presente Regolamento.
L'accesso alle immagini è consentito esclusivamente:
a) al Titolare, al Responsabile ed agli incaricati dello trattamento;
b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);
c) alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo ovvero, in casi del tutto eccezionali, all'amministratore informatico del sistema comunale (preventivamente individuato quale incaricato del trattamento dei dati);
d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte del responsabile del trattamento, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;
e) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

Articolo 8 - Obblighi degli operatori
1. L'utilizzo del brandeggio da parte degli operatori e degli incaricati al trattamento dovrà essere conforme ai limiti indicati nel presente regolamento.
2. L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici mentre esso non è ammesso nelle proprietà private.

3. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 3 e a seguito di regolare autorizzazione di volta in volta richiesta al Sindaco.
4. La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

CAPO III - TRATTAMENTO DEI DATI PERSONALI

Articolo 9 - Modalità di Raccolta e di Trattamento dei Dati

1. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di un impianto di videosorveglianza nel territorio urbano ed extra urbano, gestito dal Comune - Servizio di Polizia Locale - 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 realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
2. Presso la centrale operativa della Polizia Locale sono posizionati monitor per la visione in diretta delle immagini riprese dalle telecamere.
3. Le telecamere di cui al precedente comma 1, consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.
4. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa saranno inviati presso l'Unita di ricezione, registrazione e visione ubicata nell'Ufficio Polizia Locale. In questa sede le immagini saranno visualizzate su monitor e registrate su supporto magnetico.
5. I dati personali oggetto di trattamento sono:
- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per le finalità di cui all'art. 3 del presente Regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;
- raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.
6. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

7. Nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle richiamate disposizioni normative, 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 specifiche esigenze di ulteriore conservazione.
8. In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria l'esercente le funzioni potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai sette giorni previa richiesta al Garante per la protezione dei dati personali che, a seguito di verifica preliminare, potrà rilasciare parere favorevole.
9. Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato l´integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
10. In caso di cessazione del trattamento, i dati personali sono distrutti.

Articolo 10 - Informazioni rese al momento della raccolta
1. Il Comune, in ottemperanza a quanto disposto dal GDPR – Reg. UE n. 679/2016, dal Decreto legislativo 10 agosto 2018, n. 101, dal D.P.R., 15/01/2018 n° 15, G.U. 14/03/2018 e dal Provvedimento Garante Privacy in materia di videosorveglianza 8 aprile 2010, si obbliga ad affiggere un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.
2. Il Comune, nella persona dell'esercente le funzioni del trattamento dei dati personali, 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, ai sensi del successivo art. 15, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.
3. Gli interessati devono 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 l'Ente utilizzerà il modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita,allegato al presente Regolamento. L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui possono essere posizionate le telecamere, su cui è riportata la seguente dicitura: "Area videosorvegliata – la registrazione è effettuata dal Comune di Inveruno, per fini di sicurezza urbana, incolumità, ordine pubblico…" a seconda dell'interesse pubblico da tutelare.
4. La segnaletica deve essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.
5. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi conformi al modello allegato.

Articolo 11 - Notificazione

1. Il Comune, nella sua qualità di titolare del trattamento dei dati personali, rientrante nel campo di applicazione del presente regolamento, al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare, adempie agli obblighi di notificazione preventiva al Garante per la protezione dei dati personali, qualora ne ricorrano i presupposti, ai sensi e per gli effetti dell'art. 36 del GDPR.

Articolo 12 - Valutazione di impatto sulla protezione dei dati

1. In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), RGPD, qualora il trattamento di dati realizzato mediante il sistema di videosorveglianza comunale dia luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, l'Ente procederà ad una valutazione di impatto sulla protezione dei dati personali.
2. Parimenti si procederà nei casi in cui, il trattamento di dati realizzato mediante il sistema di videosorveglianza presenti un rischio comunque elevato per i diritti e le libertà delle persone fisiche.
3. Ai fini della valutazione d'impatto si farà riferimento all'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto come da allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 del Garante della Protezione dei Dati Personali

Articolo 13 - Altri sistemi di videosorveglianza o ulteriori strumenti di videoripresa

1. Il sistema di videosorveglianza del Comune di Inveruno potrà constare anche di Body Cam (sistemi di ripresa indossabili), Dash Cam (telecamere a bordo di veicoli di servizio) e fototrappole (telecamere mobili) da assegnare al Servizio di Polizia Locale per il loro utilizzo in situazioni di rischio operativo. Il personale del Servizio di Polizia Locale può utilizzare, per i servizi individuati dal Responsabile, delle Body Cam (telecamere posizionate direttamente sulle divise degli operatori di P.L.) e delle Dash Cam (telecamere a bordo di veicoli di servizio) in conformità alle indicazioni con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati è ricondotto nell'ambito del D.Lgs 51/2018 trattandosi di dati personali direttamente correlati all'esercizio dei compiti di polizia, di prevenzione di reati di tutela dell'ordine e della sicurezza pubblica nonché di polizia giudiziaria.
2. Il Responsabile del Servizio curerà la predisposizione di uno specifico disciplinare tecnico interno, da somministrare agli operatori di Polizia Locale che saranno dotati di microcamere, con specificazione dei casi in cui le BodyCam e le Dash Cam devono essere attivate, dei soggetti eventualmente autorizzati a disporre l'attivazione, delle operazioni autorizzate in caso di emergenza e di ogni altra misura organizzativa e tecnologica necessaria alla corretta e legittima gestione di detti dispositivi .
3. Per lo svolgimento delle attività di polizia, il Servizio di Polizia Locale potrà utilizzare fototrappole. Nello specifico al fine di:

- scoraggiare e prevenire il fenomeno dell'abbandono dei rifiuti, che comporta, oltre la compromissione del decoro urbano e l'inquinamento ambientale, anche l'esborso di considerevoli spese per la rimozione dei materiali depositati e la bonifica dei siti interessati dalle micro discariche;
- la rilevazione, prevenzione e controllo degli illeciti amministrativi e penali svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
- l'acquisizione di prove.

4. Il sistema delle fototrappole comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese e che, in relazione ai luoghi di installazione delle fototrappole, interessano i soggetti ed i mezzi di trasporto che transiteranno nelle aree interessata.
5. L'installazione delle fototrappole avviene esclusivamente da parte di personale della Polizia Locale nei luoghi pubblici in conformità all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale di volta in volta individuati.
6. L'utilizzo delle Body Cam e Dash Cam deve essere preceduto dall'accordo sindacale o dall'autorizzazione dell'Ispettorato del lavoro ai sensi dell'art. 4 della L. 300/1970.
7. Al fine di promuovere la sicurezza integrata sul territorio, recependo i contenuti del decreto legge 14/2017 convertito in legge 48/2017 "Disposizioni urgenti in materia di sicurezza delle città" ed in particolare rispetto le previsioni di cui all'art. 7 dello stesso, possono essere individuati specifici obiettivi per incrementare il controllo del territorio attraverso il concorso, sotto il profilo di sostegno strumentale, finanziario e logistico, di soggetti pubblici e privati. Tali obiettivi sono individuati nell'ambito dei "patti per l'attuazione della sicurezza urbana" di cui all'art. 5 del predetto decreto, nel rispetto delle linee guida adottate.
8. Oltre all'ipotesi di cui al comma precedente, potranno essere attivate le seguenti tipologie di sistemi integrati, previa sottoscrizione di un protocollo di gestione:
a) gestione coordinata di funzioni e servizi tramite condivisione delle immagini riprese da parte di diversi e autonomi titolari del trattamento, utilizzando le medesime infrastrutture tecnologiche;
b) collegamento telematico di diversi titolari di trattamento ad un "centro" unico gestito da soggetto terzo;
c) collegamento del sistema di videosorveglianza con la sala operativa degli organi di polizia, previa sottoscrizione di apposito "patto per l'attuazione della sicurezza urbana" di cui al comma precedente, ed espletamento delle procedure di nomina previste dal Capo II.
9. L'utilizzo di sistemi integrato di videosorveglianza, ivi compresi quelli che consentono di rendere disponibili le immagini alle Forze di Polizia, non deve essere sottoposto a verifica preliminare da parte del Garante nei casi in cui possano essere applicate, oltre alle generali misure di sicurezza (individuate dal Garante nel punto 3.3.1 del provvedimento dell'8 aprile 2010) le seguenti specifiche ulteriori misure che prevedono:
a) l'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;
b) la separazione logica delle immagini registrate dai diversi titolari.
10. Il sistema di videosorveglianza del Comune di Inveruno potrà constare anche di strumenti di lettura targhe dei veicoli, gestiti direttamente dagli operatori del Servizio di Polizia Locale come supporto nella protezione degli utenti della strada e nell'accertamento delle violazioni relative alla circolazione dei veicoli.
Il software del sistema di cui al presente comma può essere installato su una telecamera semplice o su un dispositivo specifico. La telecamera può essere posizionata su un supporto fisso e può essere utilizzata in movimento; questa scansiona le targhe e le invia al server collegato al Ministero dei Trasporti, all'IVASS e al Ministero dell'Interno. Le informazioni sulle targhe trasmesse vengono poi inviate immediatamente su dispositivo in dotazione agli operatori in servizio, per la verifica in tempo reale.

Ai sensi dell'art. 200 del D.Lgs. 285/1992 e nel rispetto delle circolari ministeriali diramate in materia, il dispositivo in oggetto ha la funzione di accertamento diretto delle violazioni, così da procedere alla contestazione immediata da parte degli operatori che ne stanno facendo uso, nel momento immediatamente successivo al transito del veicolo. Nella situazione di fatto che renda impossibile la contestazione immediata, devono essere dettagliatamente indicate nel verbale di accertamento le motivazioni che non l'hanno consentita.
11. Riguardo la conservazione dei fotogrammi si richiamano i contenuti del provvedimento del Garante della protezione dei dati personali dell'8 aprile 2010, nonché l'articolo 7 del presente Regolamento.

Articolo 14 - Diritti dell'interessato
1. In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, su presentazione di apposita istanza, ha diritto:
a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD, 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;
d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.
2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sulla home page del sito istituzionale dell'Ente alla Sezione "Privacy") ovvero al Responsabile del trattamento dei dati individuato nel Responsabile dell'Area Tecnica.
3. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
-il luogo, la data e la fascia oraria della possibile ripresa;
-l'abbigliamento indossato al momento della possibile ripresa;
-gli eventuali accessori in uso al momento della possibile ripresa;
-l'eventuale presenza di accompagnatori al momento della possibile ripresa; l'eventuale attività svolta al momento della possibile ripresa;
-eventuali ulteriori elementi utili all'identificazione dell'interessato.
4. Il responsabile della protezione dei dati dell'Ente ovvero il responsabile del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.
5. Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati

identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.
6. 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.
7. 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.
8. 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.

Articolo 15 - Sicurezza dei dati
1. I dati personali oggetto di trattamento sono custoditi ai sensi e per gli effetti del precedente art. 9.
2. I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:
a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.
A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:
a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti designati quali responsabili e incaricati del trattamento, dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le operazioni di competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà 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 immagini operazioni di cancellazione o di duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 9, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;

d) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
e) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo.

Articolo 16 - Cessazione del trattamento dei dati
1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
a) distrutti;
b) conservati per fini esclusivamente istituzionali dell'impianto attivato.

Articolo 17 - Limiti alla utilizzabilità di dati personali
1. La materia è disciplinata dall'art. 23 del GDPR.

Articolo 18 - Danni cagionati per effetto del trattamento di dati personali
1. La materia è regolamentata dall'art. 82 del GDPR. e dall'art. 15 del Decreto Legislativo 10 agosto 2018, n. 101.

Articolo 19 - Comunicazione
1. La comunicazione dei dati personali da parte del Comune di Inveruno a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria ed esclusivamente per lo svolgimento 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 dall'esercente le funzioni del trattamento dei dati personali e che operano sotto la loro diretta autorità.
3. E' 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 per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Articolo 20 - Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali
1. Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82, RGPD.
2. Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
3. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2, RGPD.

Articolo 21 - Tutela
1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 77 e ss del GDPR e 140 bis e seguenti del Decreto Legislativo 10 agosto 2018, n. 1012. 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, è l'esercente le funzioni del trattamento dei dati personali, così come individuato dal precedente art. 6.

Articolo 22 – Provvedimenti attuativi
1. Compete alla Giunta del Comune di Inveruno l'assunzione dei provvedimenti attuativi conseguenti al presente Regolamento.

Articolo 23 - Pubblicità del Regolamento
1. Copia del presente Regolamento sarà pubblicata all'albo pretorio e potrà essere reperita sul sito internet del Comune di Inveruno.

Articolo 24 – Entrata in vigore
1. Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.
2. Il presente Regolamento abroga il "*Regolamento comunale per la disciplina della videosorveglianza*" approvato con deliberazione di Consiglio Comunale n. 5 del 31/01/2006 ed ogni altra disposizione regolamentare precedente che disciplina tale materia.

Articolo 25 - Modifiche regolamentari
1. I contenuti del presente regolamento dovranno essere aggiornati nei casi di aggiornamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi nazionali e dell'UE, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali del Consiglio del Comune di Inveruno dovranno essere immediatamente recepiti.
2. Il presente regolamento è trasmesso al Garante per la protezione dei dati personali a Roma, sia a seguito della sua approvazione, sia a seguito dell'approvazione di suoi successivi ed eventuali aggiornamenti.

Allegato A
Modello Informativa

Allegato B
Elaborato planimetrico dell'ubicazione delle telecamere nel Comune di Inveruno (Mi)
