COMUNE DI PANCHIA'

PROVINCIA DI TRENTO

Regolamento del sistema di videosorveglianza.

Approvato con deliberazione del Consiglio comunale n. 10 dell'11.05.2020

Entrato in vigore il 25.05.2020

INDICE

PREMESSE

Ambito di riferimento.

Il Comune di Panchià è dotato di un sistema di videosorveglianza basato su telecamere digitali collegate tramite una rete wireless.

Il sistema di videosorveglianza è stato realizzato anche attraverso la convezione: "Val di Fiemme sicura - Videosorveglianza e controllo del territorio dei Comuni di Capriana, Valfloriana, Castello-Molina Di Fiemme, Carano, Daiano, Varena, Cavalese, Tesero, Panchià, Ziano Di Fiemme e Predazzo". La convenzione sottoscritta dai Sindaci dei Comuni partecipanti nel novembre 2015 ha consentito di accedere a vari finanziamenti e di poter collegare la rete di antenne anche a ripetitori fuori dal territorio del singolo comune. La rete intercomunale ha permesso quindi di superare le difficoltà di collegamento tipiche dei territori di montagna. La rete ha permesso anche di rendere disponibili il sistema di video sorveglianza Comunale alle forze di polizia anche quando la loro sede sia fuori dal territorio del Comune. Al fine di contenere i costi di acquisto e manutenzione si utilizza la rete anche per convogliare i dati video acquisiti dalle telecamere su un apparato di registrazione centralizzato installato nel comune di Tesero.

Il Comune di Panchià ha sottoscritto con il Comune di Tesero una convezione che definisce modalità, limiti e responsabilità nell'utilizzo dell'apparato di registrazione. La convenzione stabilisce le procedure operative atte a garantire la sicurezza e l'accesso protetto ai dati raccolti sul territorio del Comune di Panchià.

Le telecamere sono posizionate nei punti nevralgici del territorio e tramite le stesse il sistema acquisisce e registra dati relativi a immagini e video in formato digitale. I file dati contenenti video e immagini nei quali siano riconoscibili persone rientrano nella categoria dei dati personali, in particolare qualora sia possibile l'identificazione del soggetto.

Le attività legate alla videosorveglianza del territorio interferiscono quindi con il diritto alla riservatezza delle persone eventualmente presenti nell'area d'azione delle telecamere.

Questo Regolamento garantisce che il trattamento dei dati personali, effettuato, mediante sistemi di videosorveglianza di varia tipologia gestiti ed impiegati dal Comune di Panchià nel territorio comunale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Principi Generali

La Videosorveglianza in ambito pubblico si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5, GDPR e dell'art.3 del D. Lgs. n. 51/2018 e, in particolare:

- **Principio di liceità** – L'art. 5 del GDPR prescrive che i dati personali debbano essere trattati "in modo lecito, corretto e trasparente nei confronti dell'interessato". Il trattamento deve, quindi: essere conforme alla legge; perseguire uno scopo legittimo; essere necessario in una società democratica per perseguire uno scopo legittimo. Il principio di liceità, trova specificazione nell'art. 6 del GDPR, il quale prevede che ogni trattamento deve trovare fondamento in un'idonea base giuridica: la necessità del trattamento, consenso dell'interessato (da esprimersi in relazione ad "una o più specifiche finalità", e dunque non genericamente), adempimento di obblighi contrattuali, interessi vitali della persona o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati. Il trattamento di dati personali da parte di soggetti pubblici è quindi lecito anche quando 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. Art. 6, Paragrafo 1, lett. e), GDPR. **Da ciò consegue che la videosorveglianza in ambito pubblico è consentita senza necessità di consenso da parte degli interessati.**

- **Principio di necessità** – Al fine di escludere eventuali usi superflui e di evitare eccessi nella videosorveglianza e di identificare persone qualora non sia necessario i sistemi devono essere impostati in modo da poter impiegare solo i dati anonimi e riprese di insieme. I programmi (software) utilizzati per la gestione devono essere impostati in modo che i dati vengano cancellati automaticamente dopo un periodo di tempo predefinito in base e compatibile con le normative vigenti. Inoltre, per rispondere ai principi di pertinenza, adeguatezza e limitazione dei dati (art. 5, Paragrafo 1, lett. c), GDPR, la configurazione generale del sistema di videosorveglianza (apparati e programmi software) deve essere impostata in modo da ridurre al minimo l'utilizzazione di dati personali e identificativi. L'identificazione deve essere possibile solo con opportune modalità che permettano nei casi di necessità di identificare l'interessato. In questo modo si esclude il trattamento perché le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi.

- **Principio di proporzionalità** – Acquisizione, archiviazione e uso dei dati di videosorveglianza devono essere proporzionali. Nell'installazione e configurazione del sistema deve essere tenuto un bilanciamento tra l'effettiva necessità e il grado di rischio concreto per evitare di sottoporre a videosorveglianza aree nelle quali non sussistono concreti pericoli, o attività per le quali non sia necessaria un'effettiva esigenza di deterrenza. Inoltre, prima di sottoporre a videosorveglianza un'area devono essere valutate misure alternative e solo se queste siano insufficienti o inattuabili attuare la video sorveglianza. L'effettiva proporzionalità della videosorveglianza va valutata in ogni fase o modalità del trattamento e per le apparecchiature installate e posizionate per riprendere aree esterne e edifici fanno impostate modalità tali da limitare l'acquisizione alle aree effettivamente da proteggere.

- **Principio di finalità** – Ai sensi dell'art. 5, Paragrafo 1, lett. b), GDPR, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. La videosorveglianza è quindi consentita come misura complementare volta a migliorare e garantire la sicurezza urbana che il DM Interno 05/08/2008 definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."

Normativa di riferimento

Questo regolamento disciplina l'uso e la sicurezza del trattamento di dati personali, acquisiti tramite il sistema di videosorveglianza installato nel territorio del Comune di Panchià.

Per quanto non disciplinato dal questo Regolamento, si rinvia a quanto disposto dal:

- Regolamento UE Generale sulla Protezione dei Dati 2016/679 GDPR relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e alla circolazione di tali dati";
- D. Lgs. 10/08/2018 n.101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) GDPR 2016/679 27//2016.
- D. Lgs. 18/05/2018 n. 51 "Attuazione della Direttiva UE 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";
- Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008);
- Legge n. 38/2009 recante "misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori";

- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- D.P.R. 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";

  Altre fonti normative correlate alle finalità e alle attività di videosorveglianza e agli organi preposti alla attuazione e gestione della stessa.
- Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale; D.P.R. 24 luglio 1977, n.616;
- D.lgs. 31 marzo 1998, n. 112;
- D.Lgs. 18 Agosto 2000, n. 267 – TUEL;
- Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica; Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana; Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
- Circolari del Ministero dell'Interno n.558/A/421.2/70/456 in data 8 febbraio 2005, n. 558/A421.2/70/195860 in data 6 agosto 2010 e n. 558/SICPART/421.2/70/224632 in data 2.3.2012;
- Il decreto-legge 20 febbraio 2017, n. 14 convertito con la legge 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città" ha riportato alla ribalta, nell'ambito delle linee generali per la promozione della sicurezza integrata e dei patti per l'attuazione della sicurezza urbana, la necessità di prevenire e contrastare, fenomeni di criminalità diffusa e predatoria, attraverso servizi e interventi di prossimità, in particolare a vantaggio delle zone maggiormente interessate da fenomeni di degrado, anche attraverso l'installazione di sistemi di videosorveglianza. Lgs. n.51/2018 - Attuazione della direttiva (UE) 2016/680.

Definizioni

Ai fini del presente Regolamento si intende:

- **"trattamento",** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati;
- **"banca dati",** complesso organizzato di dati personali. Nel caso della videosorveglianza riguardo a dati 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;
- **"dato personale",** qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- **"dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;
- **"titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi **compreso il profilo della sicurezza;**
- **"responsabile"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

- **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- **"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 funzionario designato al coordinamento delle attività e al controllo del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del funzionario designato al coordinamento delle attività e al controllo;
- **"comunicazione"**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **"diffusione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **"dato anonimo"**, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- **"comunicazione elettronica"**, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un utente ricevente, identificato o identificabile;
- **"misure minime"**, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione;
- **"strumenti elettronici"**, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- **"autenticazione informatica"**, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- **"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;
- **"credenziali di autenticazione"**, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- **"profilo di autorizzazione"**, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché' i trattamenti ad essa consentiti;
- **"sistema di autorizzazione"**, l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
- **"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;
- **"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;

REGOLAMENTO

Art. 1. Finalità del sistema Comunale di videosorveglianza.

Il sistema di videosorveglianza del Comune di Panchià è rivolto a garantire la sicurezza urbana.

Le finalità che il Comune di Panchià intende perseguire tramite il sistema di videosorveglianza sono riferibili allo svolgimento delle funzioni istituzionali proprie dell'amministrazione comunale in particolare per:

- prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana";
- prevenire e reprimere fenomeni di degrado urbano e svolgere controlli volti ad accertare e sanzionare violazioni delle norme in materia ambientale e delle disposizioni del regolamento per la gestione integrata dei rifiuti urbani;
- vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato, dell'ordine, del decoro e della quiete pubblica;
- controllare determinate aree del territorio comunale;
- monitorare i flussi di traffico;
- verificare e calibrare il sistema di gestione centralizzata degli impianti;
- tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;
- controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico;
- attivare uno strumento operativo di protezione civile sul territorio comunale;
- acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
- 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;
- verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.
- L'utilizzo degli impianti di videosorveglianza da parte della Polizia locale, della Questura e del Comando provinciale dei Carabinieri costituisce inoltre strumento di prevenzione e di razionalizzazione dell'azione di Polizia locale, Polizia di Stato e Carabinieri sul territorio comunale, in stretto raccordo con le altre Forze dell'ordine.
- Ai sensi di quanto previsto dall'articolo 4 della legge 20 maggio 1970, n. 300, gli impianti di videosorveglianza **non possono essere utilizzati** 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 possono essere utilizzati** per l'irrogazione di sanzioni per infrazioni al codice della strada, ma esclusivamente per l'eventuale invio da parte delle centrali operative di personale con qualifica di organo di polizia stradale per le contestazioni ai sensi del codice della strada.

Le finalità sono in conformità a quanto previsto dalle norme richiamate nelle premesse del regolamento e coerenti con la cornice normativa e all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica. l'impianto di videosorveglianza del Comune di Panchià garantisce infatti la disponibilità tempestiva di immagini presso il Comune e costituisce, inoltre, uno strumento di

prevenzione e di razionalizzazione dell'azione della Polizia Locale sul territorio comunale, in stretto raccordo con le Forze dell'Ordine.

L'archivio dei dati registrati rappresenta, infatti, per il tempo di conservazione stabilito per legge, un patrimonio informativo per finalità di Polizia Giudiziaria, con eventuale informativa nei confronti dell'Autorità Giudiziaria competente a procedere in caso di rilevata commissione di reati. La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.

La possibilità di avere in tempo reale dati e immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

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.

Art. 2. Pubblicità del Regolamento.

Dopo l'approvazione questo Regolamento sarà pubblicato nell'albo pretorio e sarà reso disponibile per la consultazione nell'apposita sezione del sito internet del Comune. Il riferimento al regolamento e il link allo stesso saranno anche inseriti nella sezione "News" del sito.

Art. 3. Entrata in vigore.

Il Regolamento entrerà in vigore con l'esecutività della deliberazione di approvazione, secondo le leggi vigenti. Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.

Art. 4. Descrizione delle caratteristiche tecniche dell'impianto.

Il sistema di videosorveglianza del Comune di Panchià prevede l'uso di dispositivi di registrazione dei dati (informazioni, immagini e video). I dati registrati e gestibili sono quelli acquisiti dalle telecamere. I dati vengono incanalati verso la sede del comune mediante una rete di antenne radio in frequenza libera 2.4 5.4 GHz, opportunamente collocate su infrastrutture di proprietà comunale che consentano la visibilità ottica fra gli apparati. La rete radio in "tempo reale" è in grado di veicolare tutti i segnali video delle telecamere verso la sala controllo posta nel municipio in un locale ad esclusivo accesso degli addetti autorizzati del Comune di Panchià. Il sistema di registrazione e gestione è installato presso la sala server del Comune di Tesero.

La Sala Controllo e videosorveglianza è posizionata dentro l'ufficio della Polizia locale dove sono installate le Workstation (computer) attraverso le quali gli incaricati sono in grado di avere il completo controllo dei segnali audio, video e dati provenienti dalle telecamere installate nel territorio comunale.

Da queste postazioni è possibile visualizzare in tempo reale su monitor dedicati e accedere alle registrazioni effettuate per una facile ricostruzione degli eventi. Dalle Workstation della sala di controllo è anche possibile effettuare esportazioni. Nel caso si verifichi la necessità di comunicare alle autorità dati, video o immagini relativi ad un particolare evento/momento gli incaricati potranno esportare (sui più comuni dispositivi USB, HD USB, masterizzatori DVD) i dati richiesti dalle autorità. Questa operazione sarà eseguita garantendo l'inalterabilità dei dati mediante il sistema di autentificazione/codifica (encryption) con chiave a 128 bit tale da poter garantire l'autentificazione e

l'esigibilità in sede legale. Le telecamere impiegate sono ad alta risoluzione con OCR integrato nativo per le postazioni dove è prevista la lettura targhe.

Il sistema rispetta gli standard attualmente più diffusi rendendo così possibili ampliamenti e integrazioni sia dal punto di vista delle infrastrutture (incremento dei punti di ripresa), sia delle possibili nuove tecnologie integrabili (sistema ANPR lettura targhe, Analisi contenuto Video VCA) che al numero di centrali di controllo in questa prima fase previste per la PM e i CC.

La scelta e la posizione delle telecamere è stata fatta di concerto fra l'Amministrazione Comunale e le principali Forze dell'Ordine, prioritariamente all'esigenza di monitorare il traffico da e per il centro abitato, ma anche, le piazzole ecologiche, i parchi e le principali strutture pubbliche.

Il collegamento all'impianto di videosorveglianza può essere esteso alle Forze di Polizia che ne facciano richiesta all'Amministrazione Comunale, nei limiti e con l'osservanza delle norme contenute nel presente Regolamento ovvero disciplinate con successivo atto in conformità al quadro normativo di riferimento.

In relazione ai principi di pertinenza e di non eccedenza richiamati nelle premesse, il sistema informativo ed 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.

Art. 5. Valutazione di Impatto sulla protezione dei dati

Nel rispetto dell'art. 35, Paragrafo 3, lett. c), GDPR, 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. Allo stesso modo 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.

Art. 6. Titolare e funzionario designato del Trattamento dei dati.

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

Il funzionario, individuato dal Titolare, designato al coordinamento delle attività e al controllo del trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza è il Responsabile del servizio convenzionato di Polizia Locale, in gestione associata tra i comuni di Tesero, Panchià, Ziano di Fiemme e Predazzo.

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

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

Le competenze proprie del funzionario designato sono analiticamente disciplinate nell'atto amministrativo di nomina, con il quale il Titolare provvede alla sua individuazione.

In particolare, il funzionario designato:

- individua e nomina con propri atti gli Incaricati del trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, GDPR; detti incaricati saranno opportunamente istruiti e formati da parte del funzionario designato del trattamento con riferimento alla tutela del diritto alla

riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;

- provvede a rendere l'informativa "*minima"* agli interessati;
- verifica e controlla che il trattamento dei dati effettuato mediante sistema di videosorveglianza sia realizzato nel rispetto dei principi di cui all'art. 5 del GDPR e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;
- assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- adotta, tenendo conto delle finalità, dello stato del sistema e dei rischi connessi all'utilizzo dei dati per i diritti e le libertà delle persone, tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del GDPR;
- 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;
- 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;
- garantisce che il DPO (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;
- 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;
- 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 attività strettamente necessarie al perseguimento delle finalità istituzionali;
- 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;
- vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.
- Il funzionario incaricato si avvale del manuale delle procedure operative nelle quali sono descritte dettagliatamente tutte le procedure che egli deve svolgere per:
    - Attivare nuovi incaricati e fornire loro i profili di 'autentificazione informatica';
    - Verificare l'aggiornamento il coretto uso delle credenziali di autentificazione personali;
    - assegnare ad ogni incaricato un corretto "profilo di autorizzazione" che garantisca un accesso ai dati congruo con le mansioni e alle attività dell'incaricato;
    - Revocare credenziali nei casi previsti;
    - Modificare i profili autorizzativi;
    - Controllare i registri operativi delle attività;
    - Verificare la funzionalità tecnica dell'impianto e dei sistemi di sicurezza.
    - Altre attività tecnica e operative.

Art. 7. Incaricati del Trattamento.

Il funzionario designato procede ad individuare con proprio atto le persone fisiche incaricate del trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulti indispensabile per gli scopi perseguiti, della visione delle registrazioni.
L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato.

In ogni caso, prima dell'utilizzo degli impianti, gli incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.

Gli incaricati procedono al trattamento attenendosi alle istruzioni impartite dal funzionario designato al coordinamento delle attività e al controllo il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

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

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

Gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del funzionario designato al coordinamento delle attività e al controllo.

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

Art. 8. Modalità di Raccolta e di Trattamento dei Dati.

L'installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili) in conformità all'elenco dei siti di ripresa predisposto dall'Amministrazione Comunale.

L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle

riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.

Le telecamere consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.

Il Titolare del trattamento dei dati personali ha indicato di 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 presso gli uffici della Polizia Locale. In questa sede le immagini saranno visualizzate su monitor e registrate su supporto magnetico.

I dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per le finalità di cui all'art. 1 del presente Regolamento e resi utilizzabili in altre attività di trattamento a condizione che si tratti di attività non incompatibili con tali scopi;
- raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata al massimo, 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.

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.

In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Titolare 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.

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.

In caso di cessazione del trattamento, i dati personali sono distrutti.

Art. 9. Sicurezza dei dati.

I dati personali oggetto di trattamento sono conservati 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:

- la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
- 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, GDPR, 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:

- 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 incaricati del trattamento dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le attività di competenza;
- 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 attività di cancellazione o di duplicazione;
- per quanto riguarda il periodo di conservazione delle immagini dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
- nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette attività 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;
- gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
- la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie Wi–Fi, Wi Max, Gprs).

Il Titolare del trattamento vigila sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvede altresì ad istruire e formare gli incaricati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

Art. 10. Accesso ai dati.

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. 1 del presente Regolamento.

L'accesso alle immagini è consentito esclusivamente:

- al Titolare ed agli incaricati del trattamento;
- 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);
- 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);

- all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 13. 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 servizio convenzionato di Polizia Locale o dai suoi incaricati, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;
- 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.

Art. 11. Diritti dell'interessato.

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., GDPR, su presentazione di apposita istanza, ha diritto:

- 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;
- 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;
- di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 GDPR, 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;
- 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, GDPR.

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 ovvero al Responsabile del servizio convenzionato di Polizia Locale in qualità di funzionario incaricato.

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.

Il responsabile della protezione dei dati dell'Ente ovvero il Responsabile del servizio convenzionato di Polizia Locale 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.

Qualora, ai sensi dell'art. 15, paragrafo 3, GDPR, 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, GDPR.

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

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

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.

Art. 12. Informativa

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 utilizza lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, riportato in *fac-simile* nell'**allegato n. 1** al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010 e di seguito riportato, con indicazione, nel lato inferiore del cartello, il riferimento normativo "*Art. 13 del Regolamento europeo sulla protezione dei dati personali (RGDP 2016/679)*":

L'informativa completa sul trattamento dei dati raccolti con il sistema di videosorveglianza può essere letta nel sito internet istituzionale del Comune di Panchià, nella sezione "Privacy". L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.
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.

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

L'Ente, nella persona del Responsabile del trattamento dei dati, si obbliga ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

Art. 13. Definizione delle specifiche operative e messa in atto.

Compete alla Giunta Comunale la individuazione e l'eventuale integrazione dei siti ove posizionare le telecamere e le antenne di trasmissione. Compete alla Giunta Comunale anche la definizione delle specifiche operative come gli orari di ripresa, le zone protette da escludere dalle registrazioni, nonché la definizione di ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento.

Art. 14. Diritto al risarcimento, responsabilità - Art. 82 GDPR.

In caso di danni cagionati per effetto del trattamento di dati personali. 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, GDPR.

Il Titolare del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

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, GDPR.

Art. 15. Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale.

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, GDPR ed alle previsioni Decreto Legislativo 101/2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, 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", in attuazione della delega al Governo di cui all'art. 13, L. 163/2017.