



COMUNE di PANDINO
Provincia di Cremona

Via Castello n° 15, 26025

P.IVA 00135350197

protocollo.comune.pandino@pec.it



COMUNE DI PANDINO

REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO TRAMITE DISPOSITIVI DI ACQUISIZIONE IMMAGINI E GEOLOCALIZZAZIONE

Approvato con Deliberazione del Consiglio Comunale n. 16 del 14/05/2021

RESPONSABILE AREA POLIZIA LOCALE

[V. Comm. Mauro Dott.ssa Francesca](mailto:V.Comm.Mauro.Dott.ssa.Francesca)

0373.973340

vigili@comune.pandino.cr.it

REFERENTE PRATICA

[V. Comm. Mauro Dott.ssa Francesca](mailto:V.Comm.Mauro.Dott.ssa.Francesca)

0373.973339

vigili@comune.pandino.cr.it

Sommario

CAPO I – DISPOSIZIONI GENERALI.....	4
1. Oggetto del Regolamento.....	4
2. Definizioni.....	4
3. Norme di riferimento.....	4
4. Ambito di applicazione.....	5
5. Principi generali.....	5
6. Finalità del trattamento.....	6
CAPO II – MODALITA' DI TRATTAMENTO DEI DATI.....	8
7. Acquisizione dei dati.....	8
8. Trattamento da parte degli operatori.....	8
9. Estrazione di copia.....	8
10. Comunicazione a terzi.....	9
11. Conservazione dei dati.....	9
12. Cessazione del trattamento.....	9
13. Limitazione del trattamento.....	10
CAPO III – SOGGETTI COINVOLTI NEI TRATTAMENTI.....	11
14. Titolare del trattamento.....	11
15. Supervisor del trattamento.....	11
16. Soggetti autorizzati al trattamento dei dati personali.....	13
17. Soggetti esterni che trattano dati per conto del Titolare.....	14
18. Amministratori di Sistema.....	14
CAPO IV – MISURE DI SICUREZZA.....	16
19. Accesso fisico ai sistemi e ai luoghi.....	16
20. Accesso logico ai sistemi e ai dati.....	16
21. Sicurezza nelle trasmissioni.....	17
22. Ruoli, mansioni e responsabilità.....	17
23. Utilizzo degli strumenti e dei supporti di memorizzazione.....	18
CAPO V – OBBLIGHI DEL TITOLARE.....	19
24. Informativa.....	19
25. Diritti dell'interessato.....	19
26. Valutazione di impatto sulla protezione dei dati.....	20
27. Utilizzo in ambienti di lavoro.....	21
CAPO VI – ALTRE DISPOSIZIONI.....	22

28.	Sistemi integrati di trattamento dei dati.....	22
29.	Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale	22
30.	Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali.....	23
31.	Provvedimenti attuativi.....	23
32.	Modifiche regolamentari.....	24
33.	Entrata in vigore	24

CAPO I – DISPOSIZIONI GENERALI

1. Oggetto del Regolamento

Il presente Regolamento disciplina il trattamento dei dati personali effettuato mediante sistemi di acquisizione, registrazione, conservazione e gestione di immagini, videoriprese e informazioni relative alla localizzazione geografica delle persone fisiche, svolto in forma diretta o indiretta, dal Comune di Pandino e garantisce che lo stesso si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

In particolare il presente regolamento:

- a) definisce le modalità di utilizzo degli impianti di acquisizione immagini, videoriprese e informazioni sulla geolocalizzazione;
- b) disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti.

2. Definizioni

Ai fini del presente Regolamento si intende:

- 1) Sistema di Videosorveglianza: è un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione e in generale l'utilizzo di immagini e videoriprese relative a persone fisiche identificate o identificabili, anche indirettamente.
- 2) Sistema di Geolocalizzazione è un sistema attraverso il quale si effettua la raccolta, la registrazione, la conservazione e in generale l'utilizzo di informazioni sulla localizzazione geografica relative a persone fisiche identificate o identificabili, anche indirettamente.
- 3) Codice: è il D. Lgs. 196/2003, "Codice in materia di protezione dei dati personali".
- 4) RGPD: acronimo di "Regolamento Generale di Protezione dei Dati" - è il Regolamento UE 2016/679 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".
- 5) Titolare del trattamento: secondo l'art. 4 del RGPD è "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". Nel contesto di questo Regolamento, il titolare è il Comune di Pandino.
- 6) Supervisore: è il soggetto, designato dal Titolare, che sovrintende l'utilizzo di un sistema di gestione delle informazioni, coordinando le attività dei soggetti autorizzati al trattamento dei dati.

Per tutte le altre definizioni utilizzate in tale Regolamento si rimanda all'art. 4 del RGPD.

3. Norme di riferimento

Per tutto quanto non dettagliatamente disciplinato dal presente Regolamento, si rinvia a quanto disposto da:

- Regolamento UE Generale sulla Protezione dei Dati 2016/679 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”;
- Decreto Legislativo 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali”;
- 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”;
- DPR del 15/01/2018, n. 15, 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”;
- 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);
- Decreto Legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48, recante “Disposizioni urgenti in materia di sicurezza delle città”.

4. Ambito di applicazione

Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali effettuati tramite sistemi di acquisizione e gestione immagini, videoriprese e informazioni sulla geolocalizzazione geografica, svolti sotto la diretta titolarità del Comune di Pandino e/o da altri soggetti in contitolarità con il Titolare, all'interno del territorio del Comune di Pandino e degli altri enti con esso convenzionati.

5. Principi generali

Il trattamento di acquisizione immagini, videoriprese e informazioni sulla geolocalizzazione all'interno dell'ambito precedentemente definito si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 del 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) del RGPD. I trattamenti oggetto del presente Regolamento pertanto sono autorizzati 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) del RGPD, i sistemi di acquisizione immagini e videoriprese, 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 proporzionati 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) del 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.

6. Finalità del trattamento

L'utilizzo degli impianti di gestione e acquisizione di immagini, videoriprese e dati di geolocalizzazione è finalizzato a:

- a) protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, ai compiti di prevenzione, accertamento o repressione dei reati svolti dal Titolare, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze attribuite dalla legge;
- b) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
- c) protezione della proprietà;
- d) vigilanza sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
- e) tutela dell'ordine, del decoro e della quiete pubblica;
- f) controllo di aree specifiche del territorio qualora si renda necessario;
- g) utilizzo come strumento operativo di protezione civile sul territorio comunale;
- h) monitoraggio dei flussi di traffico;
- i) perseguimento degli obiettivi di organizzativi e di coordinamento degli interventi e delle risorse;
- j) acquisizione di prove;
- l) effettuazione di rilevazioni di tipo quantitativo e statistico.

Si rimanda all'art. 31 del presente Regolamento per la modalità di definizione delle specifiche finalità di ogni impianto installato presso il territorio su cui tale regolamento viene applicato.

CAPO II – MODALITA' DI TRATTAMENTO DEI DATI

7. Acquisizione dei dati

I dati sono acquisiti tramite strumenti idonei al perseguimento delle finalità del titolare, attraverso memorizzazione su specifici supporti installati sulle periferiche di acquisizione o trasmissione verso una centrale di acquisizione dei dati.

I sistemi di acquisizione di immagini e video sono installati in siti predefiniti dal Supervisore competente e tramite specifico atto di determinazione.

Il Supervisore competente definisce il numero e la tipologia di apparati di geolocalizzazione utilizzati in conformità con la propria autonomia organizzativa e competenza.

8. Trattamento da parte degli operatori

I dati acquisiti sono trattati da soggetti per cui sono stati definiti specifici profili di accesso, tra cui si possono prevedere:

- Visione delle immagini e delle videoriprese acquisite in tempo reale;
- Consultazione istantanea della posizione geografica degli strumenti di geolocalizzazione, anche attraverso strumenti di rappresentazione su mappe digitali;
- Estrazione dei percorsi effettuati dagli strumenti di geolocalizzazione, eventualmente in forma anonima;
- Consultazione dei dati registrati;
- Gestione dei dati acquisiti, tra cui cancellazione, estrazione di copia su supporti digitali e/o stampa su supporti analogici;
- Svolgimento di operazioni avanzate sui sistemi di acquisizione, tra cui lo spegnimento/riavvio, il blocco, l'attivazione, lo zoom, il brandeggio, il riversamento delle immagini acquisite e l'utilizzo di funzionalità evolute.

I soggetti abilitati sono debitamente autorizzati al trattamento dei dati ed istruiti per il corretto utilizzo degli strumenti e dei supporti di memorizzazione dei dati.

9. Estrazione di copia

E' consentita l'estrazione di copia dei dati acquisiti, nonché il riversamento su supporto digitale o analogico, ai fini della difesa di un diritto o del riscontro ad un'istanza di accesso, oppure per assistere la competente autorità giudiziaria o di polizia giudiziaria.

Tali attività possono essere svolte esclusivamente da soggetti appositamente autorizzati al trattamento.

I supporti digitali o analogici su cui vengono riversati i dati devono essere custoditi in sicurezza.

10. Comunicazione a terzi

Ove dovessero essere rilevate informazioni identificative di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, il Supervisore del sistema che ha acquisito i dati o un soggetto debitamente autorizzato provvederà a darne immediata comunicazione agli organi competenti.

Solo gli organi di Polizia e l'Autorità Giudiziaria potranno accedere alle informazioni raccolte, tramite consultazione presso le sedi del Titolare, trasmissione telematica o consegna di copia su supporto digitale o analogico.

I sistemi di gestione potranno essere utilizzati anche a supporto di indagini di Autorità Giudiziaria, di organi di Polizia o di Polizia Locale.

Nel caso in cui gli organi della Polizia dello Stato o della Polizia Locale, nello svolgimento di loro indagini, necessitino di disporre di informazioni ad esse collegate che sono contenute nei dati acquisiti, potranno farne richiesta scritta e motivata indirizzata al Supervisore.

11. Conservazione dei dati

I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono cancellati con modalità specificamente determinate a seconda del sistema di videosorveglianza.

Nel caso di acquisizione di dati di geolocalizzazione, i tempi di conservazione saranno predeterminati a seconda delle necessità di carattere organizzativo che hanno motivato l'utilizzo di tali strumenti, fino ad un massimo di trenta giorni, adottando idonee misure a tutela degli interessati. Decorso tale periodo, i dati registrati sono cancellati con modalità specificamente determinate a seconda del sistema di georeferenziazione.

La conservazione dei dati personali per un periodo di tempo superiore a quello indicato precedentemente è ammessa esclusivamente su specifica richiesta dell'Autorità Giudiziaria o di Polizia Giudiziaria, in relazione ad un'attività investigativa in corso. In tali casi dovrà essere informato il Supervisore competente, che darà esplicite disposizioni ai soggetti designati ad operare per tale fine.

Per situazioni non rientranti nei casi analizzati precedentemente, la conservazione dei dati personali per un tempo eccedente a quanto stabilito è subordinata ad una verifica preliminare di legittimità e necessità.

12. Cessazione del trattamento

In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali possono essere:

a) distrutti;

b) ceduti ad altro titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;

c) conservati per fini esclusivamente istituzionali dell'impianto attivato.

La cessione dei dati in violazione di quanto previsto alla precedente lett. b) o di altre disposizioni di legge in materia di trattamento dei dati personali è priva di effetti. Sono fatte salve le sanzioni previste dalla legge.

13.Limitazione del trattamento

L'interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'art. 18 del RGPD.

In tali casi i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

CAPO III – SOGGETTI COINVOLTI NEI TRATTAMENTI

14. Titolare del trattamento

Il Comune di Pandino è Titolare del trattamento dei dati personali acquisiti mediante utilizzo degli impianti di cui al presente Regolamento. A tal fine il Titolare è rappresentato dal Sindaco, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.

Il Sindaco, in qualità di rappresentante del titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti:

- a) definisce le linee organizzative per l'applicazione della normativa di settore;
- b) dispone le 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;
- c) dispone quando necessario la valutazione di impatto sulla protezione dei dati di cui all'art. 35 del RGPD ed eventualmente la consultazione preventiva al Garante per la protezione dei dati personali di cui all'art. 36 RGPD, oltre a qualsiasi altra consultazione ritenuta necessaria per il corretto trattamento dei dati, interagendo con l'autorità nei casi previsti dalla norma;
- d) designa i Supervisor del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di cui al presente regolamento, impartendo istruzioni ed assegnando compiti e responsabilità;
- e) detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti;
- f) vigila sulla puntuale osservanza delle disposizioni impartite.

15. Supervisor del trattamento

Il Comandante del Corpo di Polizia Locale del Comune di XXX, o un diverso soggetto individuato dal Sindaco, sono designati quali Supervisore del trattamento di dati personali effettuato mediante l'utilizzo degli impianti di cui al presente regolamento. La nomina è effettuata con atto del Sindaco, nel quale sono analiticamente specificati i compiti affidati. In particolare il Supervisore:

- a) individua e autorizza con propri atti i soggetti autorizzati al trattamento, definendo specificamente ruoli e responsabilità ed impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati; il Supervisore è responsabile dell'opportuna istruzione e formazione dei soggetti autorizzati, 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;
- b) quando un trattamento deve essere effettuato da soggetti esterni per conto del Titolare del trattamento, il Supervisore ricorre a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato. Il ricorso a responsabili è disciplinato da un contratto o altro atto giuridico a norma, ai sensi dell'art. 28 RGPD;

- c) provvede a rendere disponibile l'informativa "minima" agli interessati secondo quanto definito all'art. 24 del presente Regolamento;
- d) verifica e controlla che il trattamento dei dati effettuato mediante i sistemi di cui al presente regolamento, 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;
- e) assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- f) 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, il Supervisore ha la responsabilità dell'adozione di tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;
- g) 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;
- h) assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza, 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;
- i) 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) 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;
- m) 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;
- n) supporta il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD 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;
- o) 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;
- p) assiste il Titolare nell'individuazione dei siti per cui si rende necessario il ricorso all'utilizzo di sistemi di videosorveglianza e nella determinazione dei tempi di conservazione delle immagini, delle videoriprese e dei dati di geolocalizzazione;
- q) 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;

r) 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;

s) 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;

t) assicura che i soggetti autorizzati 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, vigilando sul rispetto da parte degli stessi degli obblighi di corretta e lecita acquisizione ed utilizzazione dei dati;

u) garantisce la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale autorizzato con riferimento ai trattamenti realizzati mediante gli impianti oggetto del presente regolamento, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali.

16. Soggetti autorizzati al trattamento dei dati personali

Il Supervisore del trattamento autorizza i soggetti al trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di cui al presente Regolamento. L'autorizzazione è formalizzata con atto scritto, nel quale sono analiticamente specificati i compiti affidati ai soggetti autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati. I soggetti autorizzati sono designati tenendo conto della loro esperienza, capacità e affidabilità al fine di garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

In particolare, i soggetti autorizzati devono:

a) utilizzare sempre le proprie credenziali personali per l'accesso ai sistemi informatici, garantendone la riservatezza;

b) mettere in sicurezza gli strumenti di accesso alle informazioni e gli eventuali supporti di memorizzazione assegnati, in modo da evitare che i dati trattati siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

c) mantenere la massima riservatezza sulle informazioni di cui vengano a conoscenza nell'esercizio delle loro mansioni;

d) custodire e controllare e conservare i dati personali rispettando le misure di sicurezza predisposte dall'Ente, 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;

e) evitare di creare banche dati nuove senza autorizzazione espressa del Supervisore del trattamento;

f) segnalare al Supervisore situazioni per cui, nello svolgimento delle attività assegnate, dovessero venire a conoscenza di informazioni eccedenti la propria autorizzazione al trattamento, oppure dovessero ravvisare elementi che potrebbero inficiare la sicurezza dei sistemi, dei dati trattati o dei supporti di memorizzazione;

g) fornire al Supervisore dei dati trattati 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;

h) garantire la massima collaborazione in caso di istanze avanzate da parte degli interessati, di accertamenti/ispezioni da parte dell'Autorità Garante per la protezione dei dati personali e di richieste di accesso ai dati da parte di autorità giudiziarie o di polizia giudiziaria, attenendosi alle disposizioni del Supervisore o del Titolare.

I soggetti autorizzati devono trattare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare o del Supervisore.

L'utilizzo dei dispositivi di acquisizione da parte dei soggetti autorizzati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.

In caso di sostituzione del Supervisore, persiste la validità delle autorizzazioni precedentemente attribuite, salvo che il nuovo Supervisore disponga diversamente; il nuovo Supervisore è comunque tenuto a verificare la sussistenza delle autorizzazioni precedentemente rilasciate, provvedendo al loro aggiornamento in caso di necessità.

17.Soggetti esterni che trattano dati per conto del Titolare

Il Titolare del trattamento, anche tramite il Supervisore, ha la facoltà di avvalersi di soggetti esterni, in qualità di responsabili, per lo svolgimento di attività correlate alla gestione e al funzionamento dei sistemi, che potrebbero comportare, seppur in maniera accidentale, un trattamento di dati.

Queste attività possono comprendere la manutenzione tecnica degli impianti, l'amministrazione dei sistemi informatici, il backup delle informazioni, la profilazione delle utenze che accedono ai dati, la conservazione presso proprie infrastrutture tecnologiche dei dati acquisiti e tutte le operazioni che potrebbero comportare, per loro natura, delle criticità in merito alla protezione dei dati personali.

I soggetti a cui il Titolare ricorre in qualità di responsabili devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato.

Il Titolare disciplina i trattamenti effettuati da parte del responsabile mediante contratto ovvero altro atto giuridico, specificando obblighi e responsabilità ai sensi degli artt. 28 e 29, RGPD. La regolamentazione di tali impegni può essere formalizzata dal Supervisore o altri soggetti designati.

18.Ammistratori di Sistema

Tra le mansioni assegnate ai soggetti autorizzati o ai responsabili esterni possono rientrare attività tecniche di gestione e manutenzione di sistemi elaborativi o di loro componenti.

In tali casi, devono essere esplicitate per tali soggetti, interni o esterni, le mansioni di amministrazione dei sistemi assegnate con precisa definizione dei rispettivi perimetri operativi e responsabilità.

Coloro che svolgono mansioni di amministrazione dei sistemi informatici devono essere espressamente designati da soggetti aventi titolo di rappresentare il Titolare negli specifici contesti del trattamento.

Il Supervisore redige e mantiene aggiornato l'elenco degli amministratori di sistema designati fra il personale dell'ente, oltre che l'elenco dei responsabili esterni che svolgono mansioni di amministrazione dei sistemi. Questi ultimi, a loro volta, sono tenuti a mantenere aggiornato l'elenco delle persone fisiche che operano come amministratori di sistema per conto del Titolare, che dovrà essere reso disponibile su richiesta dell'ente.

Il Supervisore e i responsabili sono tenuti, per i contesti di loro competenza e responsabilità, al rispetto delle prescrizioni specificate nel provvedimento del Garante Privacy sugli amministratori di sistema e aggiornamenti successivi.

CAPO IV – MISURE DI SICUREZZA

19. Accesso fisico ai sistemi e ai luoghi

I dati personali acquisiti mediante l'utilizzo dei sistemi di videosorveglianza di cui al presente Regolamento sono custoditi in zone ad accesso riservato.

In caso di locali interni all'ente l'accesso è consentito esclusivamente al Titolare, al Supervisore competente, ai soggetti autorizzati e ai responsabili, individuati ai sensi degli articoli 15, 16, 17 del presente Regolamento. L'accesso da parte di soggetti diversi da quelli precedentemente indicati è subordinato al rilascio, da parte del Titolare o del Supervisore, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. L'accesso avviene in presenza di soggetti autorizzati dal Supervisore. L'accesso ai locali può essere consentito esclusivamente ad incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità definite per lo specifico trattamento di dati, nonché al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali.

Il Supervisore competente impartisce idonee istruzioni atte ad evitare assunzioni o rilevamenti di dati da parte dei soggetti autorizzati all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali, garantendo la riservatezza delle informazioni.

I soggetti autorizzati vigilano sulla puntuale osservanza delle istruzioni impartite dal Supervisore e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

In caso i dati personali siano custoditi in siti esterni a seguito di specifica prestazione di servizio conferita ad un responsabile esterno, quest'ultimo è tenuto a garantire l'adozione di adeguate misure di sicurezza fisica al fine di ridurre al minimo il rischio di accesso non autorizzato ai sistemi e ai luoghi presso cui viene effettuato il trattamento.

20. Accesso logico ai sistemi e ai dati

L'accesso ai sistemi che gestiscono i dati oggetto del presente regolamento e ai dati oggetto dello specifico trattamento può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate su disposizione del Supervisore del trattamento.

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 perseguimento delle finalità definite per lo specifico trattamento di dati.

L'accesso ai dati è consentito esclusivamente:

- a) al Titolare, al Supervisore ed ai soggetti autorizzati al 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) ai responsabili incaricati della manutenzione dei sistemi, nei limiti strettamente necessari alle specifiche esigenze di funzionamento dell'impianto medesimo ovvero, in casi del tutto eccezionali, agli amministratori di sistema dell'ente specificamente designati per tale contesto (preventivamente autorizzati al trattamento dei dati);

d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso, previo accoglimento della relativa richiesta. L'accesso da parte dell'interessato sarà limitato ai soli dati che lo riguardano direttamente; al fine di evitare l'accesso ad informazioni riguardanti altri soggetti, dovranno pertanto essere utilizzati, da parte dell'ente, adeguati accorgimenti tecnici 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 ai dati 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.

21. Sicurezza nelle trasmissioni

La trasmissione attraverso reti pubbliche di comunicazioni di immagini, videoriprese e dati di geolocalizzazione acquisite tramite dispositivi sarà effettuata previa applicazione di tecniche di cifratura che ne garantiscano la riservatezza.

I Supervisor sono tenuti a disporre l'adozione di adeguati sistemi di sicurezza per garantire la riservatezza delle trasmissioni telematiche nei contesti di propria competenza e responsabilità.

22. Ruoli, mansioni e responsabilità

I Supervisor, nell'ambito delle rispettive attività di gestione dei sistemi di videosorveglianza e coordinamento dei processi organizzativi, possono avvalersi dell'operato di soggetti autorizzati e di responsabili esterni attribuendo ad essi specifici ruoli, mansioni e responsabilità, fra cui:

- a) accesso ai sistemi per la visualizzazione dei dati in tempo reale;
- b) accesso ai sistemi per la consultazione dei dati registrati;
- c) estrazione di copia dei dati in formato analogico e/o digitale e conversione in altri formati;
- d) assegnazione di strumenti elettronici idonei per la consultazione dei dati;
- e) attribuzione di specifici profili di accesso agli operatori;
- f) riversamento di immagini e videoriprese acquisite tramite supporti di memorizzazione installati su dispositivi di acquisizione;
- g) estrazione dei percorsi effettuati dagli strumenti di geolocalizzazione, eventualmente in forma anonima
- h) utilizzo di funzionalità avanzate dei dispositivi in dotazione (es. zoom, brandeggio, ecc);
- i) assegnazione di compiti manutentivi;
- j) attribuzione di mansioni di configurazione di sistemi e/o rilascio di credenziali con relativi profili di accesso;
- k) assegnazione di qualsiasi altro incarico necessario per il corretto trattamento dei dati.

Ogni specifica attribuzione di ruoli e responsabilità deve essere formalizzata e accompagnata da apposite istruzioni organizzative ed operative.

L'attribuzione di profili di accesso, di strumenti operativi nonché di funzioni correlate al trattamento di dati deve essere effettuata a seguito di valutazione dell'esperienza, capacità e affidabilità dei soggetti destinatari, al fine di garantire l'adeguata sicurezza dei sistemi e dei dati.

23.Utilizzo degli strumenti e dei supporti di memorizzazione

I soggetti autorizzati sono tenuti a garantire la custodia in sicurezza degli strumenti utilizzati e dei supporti di memorizzazione impiegati, prestando la massima attenzione durante il loro impiego e riponendoli nei luoghi destinati alla loro conservazione, in modo da ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati.

Gli strumenti assegnati che consentano l'accesso ai dati devono essere protetti da sistemi di autenticazione e non devono essere lasciati incustoditi.

Qualora la presa in carico delle immagini e delle videoriprese venga effettuata tramite riversamento dai supporti di memoria presenti negli strumenti di acquisizione, i file contenenti dati devono essere rimossi dai supporti una volta acquisiti i dati.

In caso di dismissione di supporti di memorizzazione, questi devono essere resi inutilizzabili tramite danneggiamento fisico irreparabile, in modo che non sia consentito in alcun modo il recupero dei dati trattati.

CAPO V – OBBLIGHI DEL TITOLARE

24. Informativa

Gli interessati devono essere sempre informati del trattamento effettuato dal titolare.

In particolare, nei casi di acquisizioni di immagini e videoriprese devono essere informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici.

A tal fine il titolare utilizzerà una segnaletica riportante le informazioni minime circa il Titolare del trattamento e la finalità perseguita, come prescritto dal Garante della Privacy nei provvedimenti sulla videosorveglianza.

La segnaletica deve essere collocata prima del raggio di azione dei dispositivi di acquisizione, anche nelle loro 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 dispositivi di acquisizione, in relazione alla vastità dell'area e alle modalità delle riprese, potranno essere installati più cartelli informativi.

Il cartello potrà inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificato al fine di informare se le immagini sono solo visionate o anche registrate.

L'Ente, nella persona del Supervisore, si obbliga ad informare preventivamente la comunità cittadina dell'avvio del trattamento dei dati personali effettuato tramite l'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale, tra cui il portale istituzionale.

L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

Nel caso in cui il trattamento preveda la sorveglianza di una zona di ampia dimensione, si provvederà ad informare i soggetti interessati tramite apposita diffusione sul sito istituzionale della zona soggetta al trattamento.

In caso di acquisizione di dati di geolocalizzazione, il titolare dovrà fornire agli interessati un'informativa comprensiva di tutti gli elementi contenuti nell'art 13 del RGPD e dovrà apporre sui dispositivi e sui veicoli oggetto di geolocalizzazione un'adeguata informativa semplificata di facile comprensione.

25. Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, l'interessato, dietro 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 del 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 del RGPD.

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 del RGPD ovvero al Supervisore del trattamento designato dal Titolare.

Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare le informazioni utili alla sua identificazione tramite il sistema di videosorveglianza, fra cui il luogo, la data e la fascia oraria della possibile ripresa.

Il Supervisore 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.

In caso di richiesta di accesso ai dati di geolocalizzazione, l'interessato potrà chiedere di consultare tutti i dati in possesso del titolare, fornendo tutte le informazioni necessarie per determinare specificamente i contesti che lo riguardano, come gli strumenti e i veicoli utilizzati oltre che il periodo di utilizzo.

Qualora, ai sensi dell'art. 15, paragrafo 3 del RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files i dati in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della loro acquisizione, in ossequio alla previsione di cui all'art. 15, paragrafo 4 del RGPD.

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 propri diritti 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.

26.Valutazione di impatto sulla protezione dei dati

In ossequio al disposto di cui all'art. 35 RGPD, qualora il trattamento di dati realizzato mediante i sistemi oggetto del presente regolamento possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare provvederà all'effettuazione di una valutazione di impatto sulla protezione dei dati personali.

La valutazione di impatto non verrà effettuata qualora il trattamento dovesse rientrare nell'elenco delle tipologie di trattamenti, redatto dal Garante della Privacy, per le quali non è richiesta.

27.Utilizzo in ambienti di lavoro

Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300, gli impianti di videosorveglianza e gli strumenti di rilevazione di dati di geolocalizzazione non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'ente, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

Qualsiasi utilizzo di sistemi in ambienti di lavoro deve soddisfare i principi di liceità, non eccedenza e proporzionalità.

Il titolare deve quindi attivarsi, in caso di necessità, per l'attuazione di misure di garanzia ai sensi dello Statuto dei Lavoratori.

CAPO VI – ALTRE DISPOSIZIONI

28. Sistemi integrati di trattamento dei dati

In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, è possibile il ricorso a sistemi integrati di trattamento dei dati tra diversi soggetti, pubblici e privati.

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

- a) gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, dei dati da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare i dati solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;
- b) collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 28 RGPD da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di trattamento senza consentire, tuttavia, forme di correlazione dei dati per conto di ciascun titolare;
- c) sia nelle predette ipotesi, sia nei casi in cui l'attività di trattamento venga effettuata da un solo titolare, si può anche attivare un collegamento dei sistemi di gestione con le sale o le centrali operative degli organi di polizia. L'attivazione del predetto collegamento deve essere reso noto agli interessati.

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza, quali:

- 1) adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi;
- 2) separazione logica dei dati registrati dai diversi titolari.

Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di trattamento abbiano natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il Titolare del trattamento può effettuare una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD.

29. 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 del RGPD ed alle disposizioni attuative.

30. Diritto al risarcimento, responsabilità e 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 del RGPD.

Il Titolare e/o il responsabile 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 del RGPD.

31. Provvedimenti attuativi

Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi derivanti dal presente Regolamento, fra cui l'adozione di atti che descrivano nello specifico i trattamenti di dati effettuati dal titolare, che prevedano:

- l'individuazione dei soggetti inquadrati nell'organigramma dell'ente che svolgeranno il ruolo di supervisori;
- le finalità del trattamento;
- le motivazioni dell'installazione dell'impianto;
- la sintetica descrizione del trattamento e del flusso informativo;
- l'architettura tecnologica dei sistemi di gestione dei dati;
- le misure di sicurezza adottate;
- l'eventuale necessità di effettuare una valutazione di impatto sulla protezione dei dati e l'esito;
- le categorie di destinatari a cui vengono comunicati i dati;
- i tempi di conservazione dei dati e le modalità di cancellazione;
- le modalità di comunicazione delle informazioni relative ai sistemi utilizzati

nonché la definizione di ogni ulteriore e specifico elemento ritenuto utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento.

La Giunta Comunale provvederà ad aggiornare le informazioni di cui al presente articolo con apposito provvedimento di organizzazione ogni qualvolta un trattamento subisca variazioni rilevanti.

Spetta invece ai supervisori l'adozione di appositi atti che prevedano:

- l'autorizzazione ai soggetti che tratteranno i dati, specificando per ognuno il perimetro di azione;
- la designazione dei responsabili del trattamento ai sensi dell'art. 28 RGPD che tratteranno i dati in nome e per conto del titolare;
- la designazione degli Amministratori di Sistema, con specificazione degli ambiti di operatività;
- l'elenco dei siti in cui potranno essere collocati i sistemi di acquisizione delle immagini, sulla base delle necessità rilevate e in osservanza al principio di proporzionalità;

- l'eventuale introduzione di nuovi sistemi di geolocalizzazione, le cui caratteristiche di sicurezza siano compatibili con le prescrizioni della Giunta Comunale;
- l'attuazione di tutte le misure che garantiscano la sicurezza dei dati trattati e dei sistemi implementati.

32.Modifiche regolamentari

I contenuti del presente regolamento dovranno essere aggiornati nei casi di revisione normativa in materia di trattamento dei dati personali e in materia di videosorveglianza da parte del Consiglio Comunale.

33.Entrata in vigore

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.

Il presente Regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.

ALLEGATO 1

SCHEDA TECNICO DESCRITTIVA DEL SISTEMA DI VIDEOSORVEGLIANZA

FINALITÀ DEL TRATTAMENTO
<p>L'impianto di videosorveglianza del Comune di Pandino è finalizzato a:</p> <ul style="list-style-type: none">• prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini;• 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
MOTIVAZIONE DELL'ISTALLAZIONE DELL'IMPIANTO
<p>L'utilizzo dell'impianti di videosorveglianza da parte del Comando di Polizia locale del Comune costituisce uno strumento di prevenzione e di razionalizzazione dell'azione di Polizia locale, sul territorio comunale e di raccordo con le altre Forze dell'ordine.</p> <p>Ai sensi di quanto previsto dall'articolo 4 della legge 20 maggio 1970, n. 300, l'impianto non è utilizzato per effettuare controlli sull'attività lavorativa dei dipendenti dell'Amministrazione comunale, di altre Amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.</p> <p>Non è inoltre utilizzato per l'erogazione 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.</p>
SINTETICA DESCRIZIONE DELL'IMPIANTO E DEL FLUSSO INFORMATIVO
<p>Il sistema di videosorveglianza del Comune di Pandino si compone di una rete di comunicazione dati e telecamere connesse ad un video server indipendente che consentono una registrazione automatica delle immagini e della loro conservazione posizionato presso la Sala Controllo dell'Ufficio di Polizia Locale del Comune di Pandino, con funzioni di matrice video virtuale e di archiviazione dei filmati e delle immagini da essi estrapolate. L'applicazione di gestione del sistema è installata su tale server che non è collegato ad una linea HDLSL.</p> <p>Ad oggi sono installate complessivamente n° 18 (diciotto) telecamere suddivisibili in:</p> <ul style="list-style-type: none">• n° 02 (due) fisse di tipo analogico;• n° 16 (sedici) brandeggiabile di tipo "speed-dome". <p>I siti di installazione sono dettagliatamente indicati nella documentazione allegata al presente documento.</p> <p>I segnali video delle unità di ripresa collocate sul territorio sono monitorati e raccolti da una stazione di monitoraggio e controllo, a server indipendente, installato e collocato all'interno di idoneo armadio rack chiuso da serratura, presso la Sala Controllo dell'Ufficio di Polizia Locale del Comune di Pandino dotato di porta chiusa a serratura ed all'uopo istituita e con accesso impedito ad altro personale.</p>

In tale Sede le immagini potranno essere visualizzate e immagazzinate digitalmente in personal computer dedicati ed attivabili esclusivamente con specifica password dagli autorizzati al trattamento.

Le operazioni di raccolta, modifica, consultazione, comunicazione, trasferimento, interconnessione e cancellazione dei dati personali, eseguite in sistemi di trattamento automatizzati, sono registrate su appositi FILE di LOG, e verranno conservati per un periodo non superiore a quello stabilito dal successivo punto, ed in ogni caso nel rispetto del periodo di tempo stabilito dall'Articolo 17 del Decreto del Presidente della Repubblica n° 400 del 23 Agosto 1988. (verificare)

Considerate le finalità del sistema, le immagini ed i filmati videoregistrati dall'impianto di videosorveglianza sono conservate per il periodo di tempo stabilito dalle specifiche norme di materia, presso la memoria di massa del server dedicato della Sala Controllo. Nel caso in cui si debba aderire ad una specifica richiesta investigativa che per ragioni contingibili ed urgenti può essere preventivamente prodotta in forma orale cui far seguire formale richiesta scritta, inoltrata da parte dell'Autorità Giudiziaria o di qualsiasi organo di Polizia Giudiziaria, ovvero si palesino esigenze di Polizia Stradale nonché di Pubblica Sicurezza e/o di Sicurezza Urbana, tale termine è prorogato sino alla cessazione dello stato di necessità mediante idonea disposizione di servizio da parte del Designato al trattamento come meglio specificato negli Articoli seguenti. In tali circostanze, i dati oggetto di indagine potranno essere riversati su idoneo supporto digitale e consegnati in busta chiusa al soggetto che ne abbia fatto regolare e motivata richiesta.

In relazione alle capacità di immagazzinamento delle video immagini presso il server dedicato, le immagini riprese in diretta potrebbero distruggere quelle già registrate dopo un periodo di tempo inferiore a quello indicato.

La postazione di controllo ubicata nella Sala Controllo dell'Ufficio di Polizia Locale consente la visione, in tempo reale, dei segnali video delle telecamere di videosorveglianza installate sul territorio comunale. Tale monitor è installato con modalità tali da non risultare visibile dalla zona accessibile per il pubblico. Per tale motivo l'accesso alla Sala Controllo è regolamentato da specifiche disposizioni di servizio. In particolare oltre al Titolare, al Responsabile e all'Incaricato del Trattamento dei dati, l'accesso alla Sala Controllo è consentito esclusivamente al personale tecnico della ditta addetta alla manutenzione previamente identificato e assistito durante tutte le operazioni. Altresì tale personale tecnico non ha accesso da remoto al server ma deve recarsi, sempre accompagnato, presso la Sala Controllo per la relativa manutenzione.

Le telecamere possono essere gestite, in tempo reale, dalla postazione di controllo

Gli archivi dei filmati sono conservati nello storage del server installato presso la Sala Controllo e la consultazione e l'estrapolazione degli stessi può essere effettuata dalla postazione esclusivamente dai preposti.

Le telecamere sono e potranno essere di tipo "fisso" oppure "speed – dome". La posizione delle ottiche delle telecamere e l'angolo di inquadratura sono predefinite dal Responsabile ed eseguite con l'ausilio dei tecnici della ditta incaricata alla manutenzione.

DISPOSIZIONE DEGLI IMPIANTI

Alla data di approvazione del presente allegato tecnico, telecamere della videosorveglianza ad sono in totale 18 e sono così posizionate:

nr.2 arena interna del Castello

nr.1 in via Stefano da Pandino

nr.1 in Via Rimembranze

nr.1 in Via Battisti (Oratorio)
nr.1 Via Umberto I (fontana)
nr.1 Via Umberto I (piccolo bar)
nr.1 Via umberto I (Bar Mariani)
nr.1 Via Umberto I civico 27
nr.1 Via Borgo Roldi civico 2
nr.1 Via Garibaldi civico 1 (tabaccaio)
nr.1 in Via Castello intersezione Via Circonvallazione C e B
nr. 1 in Via Circonvallazione B intersezione con Via Baracca
nr. 4 in Via bovis (Campus scolastico)
nr. 1 Piazza Vittorio Emanuele III (Bar Castello)

ALLEGATO 2

SCHEDA TECNICO DESCRITTIVA DEL SISTEMA DI RIPRESA TRAMITE "FOTO-TRAPPOLE"

FINALITÀ DEL TRATTAMENTO
<p>Le foto-trappole in dotazione al comune fanno parte del sistema di videosorveglianza già normato dal rispettivo Regolamento.</p> <p>Le finalità dell'adozione di tali sistemi di videosorveglianza sono 2:</p> <ol style="list-style-type: none">1. attività di polizia giudiziaria, per cui le finalità sono di carattere ispettivo, di prevenzione e accertamento di illeciti da parte di autorità Giudiziarie o di Polizia;2. attività di prevenzione di atti di abbandono rifiuti sul territorio cittadino. Il ricorso alla fototrappole è motivato dall'impossibilità di controllare un'ampia zona territoriale in cui si registrano ripetute azioni di abbandono di rifiuti, per cui il presidio delle forze di Polizia Locale si è rivelato inadeguato a causa dell'estensione delle zone da monitorare. <p>I trattamenti sopra indicati sono correlati alle funzioni di pubblica sicurezza dell'ente, nonché ai compiti di tutela ambientale e corretto trattamento dei rifiuti.</p>
MOTIVAZIONE DELL'ISTALLAZIONE DELL'IMPIANTO
<p>Presso il territorio comunale di Pandino nel corso degli anni si sono intensificati gli illeciti di abbandono di rifiuti presso l'intero territorio comunale. Al fine di prevenire tali comportamenti da parte di soggetti responsabili l'ente ha deciso di implementare un sistema di video sorveglianza fisso ed uno mobile. Il sistema di acquisizione di immagini tramite dispositivi mobili utilizza la strumentazione riferita ad un gruppo di "fototrappole" che possono essere posizionate in differenti località e spostate secondo le necessità.</p> <p>Previa apposizione di opportuna cartellonistica informativa sono infatti montati dispositivi atti a individuare i responsabili dell'abbandono rifiuti. La semplice presenza di informative realizzate attraverso segnaletica ben visibile svolge il ruolo di prevenzione, mentre la raccolta delle immagini mira a individuare i responsabili.</p> <p>Il Comune ha già in essere un apposito regolamento per il trattamento dati personali derivato dal sistema di raccolta immagini. Il responsabile dell'intero sistema è il Comandante di Polizia Locale del Comune.</p> <p>Il trattamento consiste dunque nell'attivazione di fototrappole provviste di batteria autonoma ricaricabile a sensori infrarossi, che vengono posizionate sul territorio comunale al fine di:</p> <ul style="list-style-type: none">• prevenire e reprimere eventuali atti di abbandono di rifiuti nelle aree pubbliche;• prevenire eventuali atti di vandalismo o danneggiamento al patrimonio comunale;• acquisire prove per attività di polizia giudiziaria. <p>I risultati attesi sono quelli di ridurre comportamenti illeciti da parte di soggetti che compiono reati, azioni di danneggiamento al patrimonio comunale e di abbandono rifiuti.</p> <p>L'utilizzo di tali soluzioni sarà limitato al territorio comunale, in zone per cui altri strumenti di controllo si siano rivelati inefficaci.</p>
SINTETICA DESCRIZIONE DELL'IMPIANTO E DEL FLUSSO INFORMATIVO
<p>Le fototrappole in dotazione alla data della redazione della presente scheda tecnica si compone di due apparecchi in grado di registrare foto e video su micro SD con sistema ad infrarossi dotato di 34 LED. Ha inoltre le seguenti caratteristiche:</p> <ul style="list-style-type: none">- Registrazione video in 1080 Full HD- Alimentazione a batteria con 40 giorni di autonoma- Collegamento Cloud accessibile da app compatibile con gli smartphone in dotazione- Impermeabilità IP66

- Dotata di doppia serratura
- Con password di protezione
- Risoluzione foto 10 MP interpolabile fino a 24 MP (10-16-24 MPX)
- In grado di scattare fino a 3 foto in sequenza
- Sovrascrizione automatica delle immagini
- Illuminazione notturna fino a 15 metri
- Angolo di ripresa 57 gradi
- Lunghezza video fino a 180 secondi
- Tempo di attivazione inferiore al secondo
- 32 gb di memoria
- Immagini diurne a colori e in notturna in bianco e nero
- Registrazione audio integrata

CONSERVAZIONE DEI DATI

I dati personali registrati mediante l'utilizzo delle fototrappole di cui alla presente scheda tecnica sono conservati per un periodo di tempo non superiore ai 7 giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono cancellati dagli agenti in servizio con modalità specificamente determinate dal sistema stesso.

Nel caso di acquisizione di dati di geolocalizzazione, i tempi di conservazione saranno predeterminati a seconda delle necessità di carattere organizzativo che hanno motivato l'utilizzo di tali strumenti, fino ad un massimo di trenta giorni, adottando idonee misure a tutela degli interessati. Decorso tale periodo, i dati registrati sono cancellati con modalità specificamente determinate a seconda del sistema di georeferenziazione.