



PROVINCIA
DI PESCARA

REGOLAMENTO PER DISPOSITIVI DI ACQUISIZIONE IMMAGINI E TRATTAMENTO DEI DATI

ANNO 2025

Sommario

CAPO I – DISPOSIZIONI GENERALI.....	4
1. Oggetto del Regolamento	4
2. Definizioni	4
3. Norme e linee guida di riferimento.....	6
4. Ambito di applicazione.....	6
5. Principi generali	7
6. Finalità del trattamento e base giuridica	8
CAPO II – SOGGETTI COINVOLTI NEI TRATTAMENTI.....	9
7. Titolare del trattamento	9
8. Supervisor del trattamento	9
9. Soggetti autorizzati al trattamento dei dati personali.....	10
10. Soggetti esterni che trattano dati per conto del Titolare	12
11. Amministratori di Sistema	12
CAPO III – MODALITA' DI TRATTAMENTO DEI DATI	13
12. Acquisizione dei dati	13
13. Trattamento da parte degli operatori.....	14
14. Estrazione di copia.....	15
15. Comunicazione a terzi	15
16. Conservazione dei dati	15
17. Cessazione del trattamento	16
18. Accesso ai filmati.....	16
CAPO IV – MISURE DI SICUREZZA.....	16
19. Accesso fisico ai sistemi e ai luoghi	16
20. Accesso logico ai sistemi e ai dati	17
21. Sicurezza nelle trasmissioni	18
22. Ruoli, mansioni e responsabilità	19
23. Utilizzo degli strumenti e dei supporti di memorizzazione	19
24. Specificità per Body Cams, Dash Cams, video/fototrappole, foto/telecamere su droni e telecamera mobile con riconoscimento alfanumerico di targhe di veicoli..	Errore. Il segnalibro non è definito.
CAPO V – OBBLIGHI DEL TITOLARE	20
25. Informativa	20
26. Diritti dell'interessato.....	21
27. Valutazione di impatto sulla protezione dei dati	22

28.	Utilizzo in ambienti di lavoro	22
CAPO VI – ALTRE DISPOSIZIONI.....		23
29.	Sistemi integrati di trattamento dei dati.....	23
30.	Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale	23
31.	Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali.....	24
32.	Provvedimenti attuativi	24
33.	Modifiche regolamentari	25
34.	Entrata in vigore e norme di rinvio	25

CAPO I – DISPOSIZIONI GENERALI

1.Oggetto del Regolamento

1.Le immagini, qualora rendano le persone identificate o identificabili, costituiscono dati personali: in tali casi detti sistemi incidono sul diritto delle persone alla propria riservatezza.

2.Il presente Regolamento disciplina le modalità di raccolta, gestione e conservazione dei dati personali mediante sistemi di videosorveglianza ed in generale ogni trattamento dei dati personali effettuato mediante sistemi di acquisizione, registrazione, conservazione e gestione di immagini, audio-immagini, videoriprese e informazioni relative ad esse e riguardanti le persone fisiche coinvolte, svolto in forma diretta o indiretta, dall'Ente Provincia di Pescara.

3.Il presente Regolamento garantisce altresì 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.

4.In particolare, il presente regolamento:

- a) definisce le modalità di utilizzo degli impianti di acquisizione immagini, videoriprese e informazioni ad esse relative (es. targhe);
- 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

1.Ai fini del presente Regolamento si intende:

- 1) per "dato personale", qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 2) per "trattamento", qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 3) per "banca di dati", il complesso di dati personali, formatosi presso apparecchiature di registrazione e ripresa video, che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;
- 4) 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.
- 5) Codice: è il D. Lgs. 196/2003, "Codice in materia di protezione dei dati personali".

- 6) 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”.
- 7) 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 l’Ente Provincia di Pescara (di seguito anche semplicemente “Ente”).
- 8) Supervisore(Responsabile del Trattamento): è il soggetto (o più soggetti), designato dal Titolare, che sovrintende l’utilizzo di un sistema di gestione delle informazioni, coordinando le attività dei soggetti autorizzati al trattamento dei dati.
- 9) Responsabile della Protezione dei Dati: è una figura prevista dall’art. 37 del Regolamento UE 2016/679. Si tratta di un soggetto designato dal Titolare per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all’applicazione del Regolamento medesimo. Cooperava con l’Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento);
- 10) Interessato: la persona fisica cui si riferiscono i dati personali oggetto di trattamento.
- 11) per “incaricato” o “autorizzato”, la persona fisica che abbia accesso a dati personali e agisca sotto l’autorità del titolare o del responsabile del trattamento;
- 12) per “terzo”, la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che non sia l’interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l’autorità diretta del titolare o del responsabile;
- 13) per “violazione dei dati personali”, la violazione di sicurezza che comporta accidentalmente o in modo illecito l’accesso, la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati personali trasmessi, conservati o comunque trattati;
- 14) per “comunicazione”, il dare conoscenza dei dati personali a soggetti determinati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- 15) per “diffusione”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- 16) per “dato anonimo”, il dato che in origine, per le modalità di inquadratura o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- 17) per “blocco”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- 18) per sicurezza urbana si deve intendere la tutela della sicurezza pubblica, in quanto attività di prevenzione e repressione dei reati, con esclusione delle funzioni di polizia amministrativa (art. 6 del D.L. 23 febbraio 2009, n. 11)

2. Ai fini delle definizioni di cui al presente Regolamento si deve fare riferimento all’art. 4 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e all’art 2 del D. lgs 51/2018 relativo 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.

3. Norme e linee guida di riferimento

1. 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” e successive modifiche;
- 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 Legislativo 18 maggio 2018, n. 51, “Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti 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), nonché il provvedimento a carattere generale 29.11.2000, il decalogo delle regole per non violare la privacy ed il provvedimento a carattere generale 29.04.2004;
- Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivo video adottato il 29 gennaio 2020 dal Comitato Europeo per la protezione dei dati (European Data Protection Board – EDPB);
- Legge 20 maggio 1970, n. 300, “Statuto dei Lavoratori”;
- Ispettorato nazionale del lavoro, circolare n. 2/2016 del 7.11.2016

4. Ambito di applicazione

1. Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali effettuati tramite sistemi di acquisizione e gestione immagini, audio, svolti sotto la diretta titolarità dell'Ente e/o da altri soggetti in contitolarità con il Titolare, all'interno del territorio dell'Ente (ed eventualmente degli altri enti con esso convenzionati).

5.Principi generali

1. Il trattamento di acquisizione immagini, videoriprese all'interno dell'ambito precedentemente definito si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 del RGPD e, in particolare:

- **Principio di liceità** – Il trattamento di dati personali per mezzo di sistemi di videosorveglianza 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 rispondono a detto principio e 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 nei sistemi di videosorveglianza è escluso ogni uso superfluo e sono evitati eccessi e ridondanze.
- **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. A tal riguardo si dà atto che detta valutazione di proporzionalità verrà effettuata dall'Ente su tutto il territorio provinciale e che gli impianti di videosorveglianza, laddove previsti, sono stati o saranno adottati solo se altre misure siano state previamente e ponderatamente valutate insufficienti o inattuabili (es. controlli da parte di addetti di Polizia Locale, posti di blocco, sistemi di allarme, misure di protezione degli ingressi) per il raggiungimento delle finalità indicate. In ogni caso l'Ente garantisce che il trattamento viene effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da controllare e/o 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 sul territorio.

6.Finalità del trattamento e base giuridica

1. Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza (Body Cams, Dash Cams, video/fototrappole, foto/telecamere su droni e telecamera mobile e fisse con riconoscimento alfanumerico di targhe di veicoli) sono conformi alle funzioni istituzionali attribuite alla Provincia di Pescara e alla sua Polizia Locale dalle leggi, nazionali e regionali, nonché dallo Statuto provinciale e dai Regolamenti provinciali vigenti.

2. Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato per le seguenti finalità:

- a. presidiare e tutelare il patrimonio provinciale, le aree adiacenti ad uffici od immobili provinciali, oltre a particolari e specifici siti provinciali;
- b. tutelare la sicurezza del territorio e la pubblica sicurezza;
- c. tutelare e monitorare la sicurezza stradale, controllando la circolazione lungo le strade del territorio provinciale e rilevare infrazioni;
- d. tutelare l'ambiente, per prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado e abbandono di rifiuti e svolgere i controlli volti ad accertare e sanzionare le violazioni delle norme contenute nel Testo Unico Ambientale, nei regolamenti locali in genere e nelle ordinanze sindacali;
- e. vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
- f. tutelare l'ordine, il decoro e la quiete pubblica;
- g. controllare aree specifiche del territorio provinciale;
- h. tutelare la sicurezza degli agenti di polizia locale.

3. Il sistema di videosorveglianza comporta il trattamento di dati personali rilevati mediante le riprese video che, in relazione ai luoghi di installazione delle telecamere, interessino i soggetti ed i mezzi di trasporto che abbiano a transitare nell'area attenzionata.

4. La Provincia di Pescara – Polizia Locale promuove ed attua, per la parte di competenza, politiche di controllo del territorio integrate con organi istituzionalmente preposti alla tutela della sicurezza e dell'ordine pubblico. A tal fine la Provincia di Pescara – Polizia Locale, previa intesa o su richiesta delle autorità di pubblica sicurezza o degli altri organi di polizia, può disporre l'utilizzo degli impianti provinciali di videosorveglianza anche ai fini di prevenzione e repressione di atti delittuosi. I dati così raccolti vengono utilizzati esclusivamente dalle autorità ed organi anzidetti.

5. Conformemente a quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300 è vietato, e pertanto escluso, l'uso degli impianti di videosorveglianza per effettuare controlli a distanza sull'attività lavorativa dei dipendenti dell'amministrazione, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

CAPO II – SOGGETTI COINVOLTI NEI TRATTAMENTI

7. Titolare del trattamento

1. L'Ente Provincia di Pescara 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 Presidente della Provincia pro tempore, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.

2. Il Titolare deve garantire il rispetto degli obblighi di sicurezza di cui all'art. 32 del RGPD, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

8. Supervisor del trattamento

1. Il Dirigente del Settore Tecnico I, o un diverso soggetto individuato dal Presidente della Provincia, è designato quale Supervisore (Responsabile) del trattamento di dati personali effettuato mediante l'utilizzo degli impianti di cui al presente regolamento. La nomina è effettuata con atto del Presidente della Provincia, nel quale sono analiticamente specificati i compiti affidati. In particolare, il Supervisore (Responsabile del trattamento) nel rispetto della normativa vigente in tema di trattamento dei dati personali, ivi incluso il profilo della sicurezza, e delle disposizioni del presente Regolamento:

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" e "di secondo livello" agli interessati secondo quanto definito all'art. 24 del presente Regolamento;

d) procede al trattamento attenendosi alle presenti istruzioni;

e) vigila, anche tramite verifiche periodiche, sulla puntuale osservanza delle disposizioni previste dalla normativa vigente e delle presenti istruzioni da parte del personale autorizzato;

f) vigila, anche tramite verifiche periodiche, sull'operato da parte di eventuali responsabili (aziende esterne/incaricati esterni);

g) sovrintende all'accesso per la manutenzione e riparazione degli impianti.

2. Il Responsabile del trattamento impartisce idonee istruzioni atte ad evitare l'assunzione o il rilevamento di dati da parte di personale addetto alle manutenzioni o pulizie.

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

4. Il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 25 del D.Lgs. n. 51/2018, 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.

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

6. Il Responsabile del trattamento assiste il Titolare ed il Responsabile della Protezione dei Dati (RPD/DPO) 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 art. 33 e 34 del RGPD.

7. Il Responsabile del trattamento assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 23 del D.Lgs. n. 51/2018.

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

9. Il Responsabile del trattamento garantisce che il Responsabile della Protezione dei Dati (RDP/DPO), 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.

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

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

12. Il Responsabile del trattamento può ricorrere a ulteriori Responsabili solo previa autorizzazione del Titolare.

9. Soggetti autorizzati al trattamento dei dati personali

1. 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.

2. In particolare, i soggetti autorizzati devono:

- a) utilizzare sempre le proprie credenziali personali per l'accesso ai sistemi informatici, garantendone la riservatezza; i sistemi devono garantire la registrazione degli accessi ed il tracciamento;
- 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.

3. I soggetti autorizzati, a cui viene impartita apposita formazione, devono trattare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare o del Supervisore.

4. La gestione e l'utilizzo dei sistemi di videosorveglianza aventi per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è riservata agli organi di Polizia Locale, aventi qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del codice di procedura penale.

5. 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 nonché alle specifiche istruzioni impartite.

6. La visione delle immagini registrate è consentita, oltre agli autorizzati, anche a chi esercita funzioni di polizia giudiziaria, ed al personale esterno addetto alla manutenzione ed alle riparazioni, quest'ultimo sempre previa autorizzazione del Titolare. Ciascun autorizzato deve utilizzare le proprie credenziali, composte da nome utente e password; la password è personale e deve rimanere nota al solo titolare delle credenziali.

7. L'accesso alla sala di controllo/banca dati è consentito esclusivamente al personale designato quale incaricato del trattamento.

8. Eventuali accessi di persone diverse da quelle sopra indicate, devono essere autorizzate in forma scritta dal Responsabile del Trattamento.

9. Possono essere autorizzati solo incaricati di servizi rientranti nei compiti istituzionali dell'Ente di appartenenza e per scopi connessi al presente regolamento, nonché il personale addetto a manutenzione di impianti presenti nella sala di controllo, o addetto ai servizi di pulizia.

10. 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.

10. Soggetti esterni che trattano dati per conto del Titolare

1. 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.

2. 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.

3. 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.

4. 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.

5. Il Supervisore aggiorna periodicamente la lista dei responsabili esterni del trattamento.

11. Amministratori di Sistema

1. 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.

2. 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.

3. 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.

4. 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.

5. 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 III – MODALITA' DI TRATTAMENTO DEI DATI

12. Acquisizione dei dati

1. 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.

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

- a. videosorveglianza tramite telecamere e fotocamere;
- b. videosorveglianza con riconoscimento targhe;
- c. telecamere a bordo di veicoli di servizio (dash cams);
- d. telecamere indossabili (body cams) utilizzate dalla Polizia Locale durante le operazioni;
- e. telecamere e fotocamere montate a bordo di droni radiocomandati.

3. In ogni caso, le modalità di trattamento e di conservazione dovranno rispettare quanto disposto dalla vigente normativa, ed in particolare i dati personali oggetto di trattamento dovranno essere pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, per poi essere cancellati.

13. Specificità per Body Cams, Dash Cams, video/fototrappole, foto/telecamere su droni e telecamera mobile con riconoscimento alfanumerico di targhe di veicoli

1. Gli operatori di Polizia Locale possono utilizzare, per i servizi esterni, delle Body Cams, delle Dash Cams e telecamere mobili per il riconoscimento alfanumerico di targhe di veicoli in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016, prot. n. 49612, ed al parere preventivo pubblicato il 31/7/2014, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati è ricondotto nell'ambito del D.Lgs. n. 51/2018, trattandosi di "dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica nonché di polizia giudiziaria".

2. Gli operatori di Polizia Locale possono utilizzare le riprese tramite droni, per visualizzare aree non facilmente accessibili, o per avere una visione alternativa (aerea) dello scenario operativo (a titolo esemplificativo di un sinistro) nonché la tutela della sicurezza degli astanti o degli operatori oppure, il comprovare il corretto svolgimento delle attività istituzionali, nei casi di particolare criticità. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D.Lgs. n. 51/2018 che esimano il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.

3. Gli apparati "Telecamere modulari" (video/fototrappole) vengono posizionati secondo necessità, esclusivamente nei luoghi teatro di presunti illeciti penali o amministrativi, quando questi ultimi non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D.Lgs. n. 51/2018 che esimano il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica, per l'informativa agli utenti frequentatori di dette aree.

4. Le video/fotocamere e le schede di memoria di cui sono dotate sono contraddistinte da un numero seriale che deve essere annotato in apposito registro recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del dipendente che firmerà la presa in carico e la restituzione. La scheda di memoria, all'atto della consegna ai singoli operatori, non deve contenere alcun dato archiviato.

5. Spetta all'ufficiale di Polizia Giudiziaria che impiega direttamente la pattuglia o in mancanza al Comandante o al Capo Pattuglia di impartire l'ordine di attivazione dei dispositivi, in relazione all'evolversi degli scenari di sicurezza e ordine pubblico che facciano presupporre la criticità. Il medesimo dispone la cessazione delle riprese, che potranno essere riattivate ogni qualvolta lo stesso ne ravvisi la necessità.

6. Al termine del servizio gli operatori interessati, previa compilazione di un foglio di consegna, affidano tutta la documentazione video realizzata al dipendente in servizio presso il Comando.

7. Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza delle situazioni descritte al precedente comma 3.

8. Il trattamento dei dati personali effettuati con tali sistemi di ripresa deve rispettare i principi di cui all'art. 5.

14. Trattamento da parte degli operatori

1. 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 o da remoto;
- 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.

2. 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.

3. I dati personali oggetto di trattamento, effettuato con strumenti elettronici nel rispetto delle misure di sicurezza indicate dalla normativa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, sono:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per le finalità indicate nel presente Regolamento e resi utilizzabili per operazioni compatibili con tali scopi;
- c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;

15.Estrazione di copia

- 1.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, per assistere la competente autorità giudiziaria o di polizia giudiziaria o per rilevare infrazioni.
- 2.Tali attività possono essere svolte esclusivamente da soggetti appositamente autorizzati al trattamento.
- 3.I supporti digitali o analogici su cui vengono riversati i dati devono essere custoditi in sicurezza.

16.Comunicazione a terzi

- 1.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.
- 2.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.
- 3.I sistemi di gestione potranno essere utilizzati anche a supporto di indagini di Autorità Giudiziaria, di organi di Polizia o di Polizia Locale.
- 4.Nel caso in cui gli organi della Polizia dello Stato o della Polizia Locale, ed in generale gli organi deputati alla pubblica sicurezza, nello svolgimento di loro indagini e/o altre attività, necessitino di disporre di informazioni ad esse collegate che sono contenute nei dati acquisiti, potranno farne richiesta scritta e motivata indirizzata al Supervisore sottoscritta dal richiedente e previa identificazione.
- 5.Ogni attività effettuata deve essere tracciata.

17.Conservazione dei dati

- 1.I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conservati per il tempo necessario al perseguimento delle finalità perseguite ed in ogni caso entro i termini previsti dalla legge. Qualora, e solo per diverse comprovate esigenze, documentate caso per caso e rispondenti alle finalità istituzionali perseguite dall'Ente, sia necessario prolungare i termini di conservazione, deve esserne rilasciata ampia motivazione. Detta documentazione, a giustificazione di un termine di conservazione più lungo, deve essere conservata.
- 2.Decorso il periodo di conservazione prestabilito, i dati registrati sono cancellati con modalità specificamente determinate a seconda del sistema di videosorveglianza.
- 3.La conservazione dei dati personali per un periodo di tempo superiore a quelli indicati precedentemente è ammessa altresì su specifica richiesta dell'Autorità Giudiziaria o di Polizia Giudiziaria, in relazione ad un'attività investigativa, ispettiva o repressiva in corso. In tali casi dovrà essere informato il Supervisore competente, che darà esplicite disposizioni ai soggetti designati ad operare per tale fine.
- 4.Per situazioni non rientranti nei casi analizzati precedentemente, la conservazione dei dati personali per un tempo eccedente a quanto stabilito è sempre subordinata ad una verifica preliminare di legittimità e necessità, il cui esito deve essere ampiamente documentato ed archiviato, a giustificazione della deroga temporale.
- 5.La conservazione dei dati deve essere effettuata nel rispetto delle misure di sicurezza previste dalla normativa vigente.

18.Cessazione del trattamento

1.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 e se previsto da norme di legge o di regolamento;
- c) conservati su richiesta di un'Autorità, per legge e a fini esclusivamente istituzionali.

2.La cessazione di trattamenti di dati in ogni caso deve essere conforme alle disposizioni del RGPD.

19.Accesso ai filmati

1.Al di fuori dei diritti dell'interessato e di quanto specificato nell'art. 20 del presente Regolamento, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente.

2.Ogni richiesta dovrà essere indirizzata al Supervisore designato.

3.Non è consentito fornire direttamente ai cittadini copia delle immagini.

4.Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, i filmati possono essere richiesti ed acquisiti dall'organo di polizia stradale che ha proceduto ai rilievi e in capo al quale è l'istruttoria relativa all'incidente.

5.Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'Art. 391-quater c.p.p., può acquisire copia digitale dei filmati della videosorveglianza presentando specifica richiesta al Supervisore. In tal caso il difensore potrà presentare la richiesta motivata e provvedere alle spese per il rilascio di copia digitale dei filmati della videosorveglianza, riversato su apposito supporto. Salvo l'ipotesi di conservazione per diverse finalità, i dati si intendono disponibili per i normali tempi di conservazione.

6.Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al Supervisore che i filmati siano conservati oltre i termini di Legge, per essere messi a disposizione dell'organo di polizia procedente. La richiesta deve comunque pervenire entro i termini di conservazione previsti. Spetterà all'organo di polizia in questione procedere a formale richiesta di acquisizione dei filmati.

7.In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal Supervisore dovrà tenere traccia delle operazioni eseguite.

CAPO IV – MISURE DI SICUREZZA

20.Accesso fisico ai sistemi e ai luoghi

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

2.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.

3. 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.

4. 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.

5. 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.

21. Accesso logico ai sistemi e ai dati

1. 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.

2. 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.

3. 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 laddove ne sussistano i presupposti. 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;

f) agli altri enti e/o organi di sicurezza pubblica, previo accordo scritto, ed agli altri casi specificamente previsti al precedente articolo 13, come disposto dal presente regolamento.

22. Sicurezza nelle trasmissioni

1. La trasmissione attraverso reti pubbliche di comunicazioni di immagini, video e/o audio-riprese acquisite tramite dispositivi sarà effettuata previa applicazione di tecniche di cifratura che ne garantiscano la riservatezza.

2. 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 nonché garantire la separazione della rete di videosorveglianza da altre reti.

3. Verranno tenute in considerazione le seguenti recenti raccomandazioni dell'Agenzia per la Cibersicurezza Nazionale (ACN) per ridurre i rischi di attacchi informatici ai quali sono esposti i servizi remoti:

1. Formazione continua del personale su sicurezza informatica e riconoscimento di tentativi di attacco.
2. Impostazione di password robuste e univoche, con gestione centralizzata delle credenziali.
3. Applicazione rigorosa della politica del Least Privilege, limitando gli accessi solo al personale e ai sistemi strettamente necessari.
4. Aggiornamento tempestivo e continuo di firmware, software e patch di sicurezza per tutti i dispositivi e servizi.
5. Utilizzo obbligatorio di autenticazione multifattoriale (MFA) per ogni accesso remoto.
6. Segmentazione di rete e isolamento dei sistemi critici, utilizzando ad esempio VLAN o subnet fisiche dedicate.
7. Impiego di VPN aziendali sicure per tutti gli accessi remoti, vietando l'esposizione diretta di servizi (RDP, SSH, VNC ecc.) su Internet.
8. Disabilitazione di servizi non necessari e chiusura delle porte non utilizzate.
9. Implementazione di firewall con regole restrittive e sistemi di prevenzione intrusioni (IPS/IDS).
10. Monitoraggio continuo e centralizzato degli accessi e dei log tramite soluzioni SIEM.
11. Applicazione di politiche di controllo accessi basate su ruolo (RBAC) e revisione periodica delle autorizzazioni.
12. Adozione di sistemi di protezione avanzata, come endpoint detection and response (EDR) e antivirus aggiornati.
13. Configurazione di sistemi di notifica e allarme per accessi sospetti o anomalie di rete.
14. Adozione di un Incident Response Plan (IRP) formalizzato e testato, per gestire rapidamente e efficacemente eventuali incidenti di sicurezza.
15. Implementazione di geofencing o whitelist IP per limitare gli accessi da aree geografiche o indirizzi IP non autorizzati in particolare per sistemi critici.

16. Utilizzo di DNS sinkhole o firewall DNS per bloccare domini malevoli noti.
17. Analisi e test di vulnerabilità periodici, inclusi penetration test sui servizi esposti.
18. Implementazione di soluzioni di Zero Trust Network Access (ZTNA) per una verifica continua delle identità e dei dispositivi.
19. Backup regolari e sicuri delle configurazioni e dei dati critici per permettere il rapido ripristino in caso di compromissione.
20. Adozione di policy di sicurezza documentate e audit periodici di conformità normativa.

23. Ruoli, mansioni e responsabilità

1. 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) utilizzo di funzionalità avanzate dei dispositivi in dotazione (es. zoom, brandeggio, ecc);
- h) assegnazione di compiti manutentivi;
- i) attribuzione di mansioni di configurazione di sistemi e/o rilascio di credenziali con relativi profili di accesso;
- j) assegnazione di qualsiasi altro incarico necessario per il corretto trattamento dei dati.

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

3. 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, e previa adeguata formazione, al fine di garantire l'adeguata sicurezza dei sistemi e dei dati.

24. Utilizzo degli strumenti e dei supporti di memorizzazione

1. 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.

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

3. 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.

4. 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

25. Informativa

1. Gli interessati devono essere sempre informati del trattamento effettuato dal Titolare.

2. 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.

3. A tal fine il Titolare utilizzerà una informativa cosiddetta di “primo” e di “secondo livello”.

4. Quanto all’informativa di “primo livello”, finalizzata per relazionarsi in modo primario e diretto con l’interessato, il Titolare utilizzerà un cartello di avvertimento per dare una visione di insieme del trattamento previsto in modo facilmente visibile, comprensibile e chiaramente leggibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno. Il cartello è posizionato prima di entrare nell’area monitorata. Detto cartello riporterà le informazioni più importanti, comprese quelle di maggior impatto per l’interessato (es. finalità e base giuridica del trattamento, identità del Titolare, i dati di contatto del Responsabile della Protezione dei Dati e i diritti degli interessati, il periodo di conservazione, le modalità di trasmissione). Verrà inoltre riportato anche il luogo ove l’interessato potrà prendere visione dell’informativa per esteso.

5. In presenza di più dispositivi di acquisizione, in relazione alla vastità dell’area e alle modalità delle riprese, potranno essere installati più cartelli informativi.

6. 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.

7. Quanto all’informativa di “secondo livello”, essa verrà resa disponibile in luogo facilmente accessibile all’interessato, come il sito istituzionale dell’Ente, e dovrà contenere tutte le informazioni obbligatorie previste dall’art. 13 RGPD. Nel medesimo luogo sarà resa disponibile altresì la localizzazione delle telecamere presenti sul territorio provinciale.

8. 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, anche attraverso una sua mappatura, 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.

9. 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.

10. 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.

26. Diritti dell'interessato

1. In relazione al trattamento di dati personali che lo riguardano, oltre alla dovuta informativa, 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 nelle modalità previste dal presente Regolamento;

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 e di tutto quanto previsto ex art. 13 RGPD;

c) di richiedere la cancellazione nei casi previsti dal Regolamento UE 2016/679 qualora sussista uno dei motivi di cui all'art. 17 del RGPD, nonché 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, nei casi previsti dal Regolamento UE 2016/679, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21 del RGPD. Il Supervisore informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti.

e) 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.

2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4 del RGPD ovvero al Supervisore del trattamento designato dal Titolare, che, laddove necessario, si consulterà con il Responsabile della Protezione dei Dati.

3. 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.

4. 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, 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.

5. Qualora il Supervisore non sia in grado di identificare l'interessato o in caso di richieste eccessive o manifestamente infondate da parte dell'interessato, il Supervisore – previa adeguata motivazione – informerà l'interessato dell'impossibilità di dare seguito alla richiesta.

6.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.

7.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.

8.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.

9.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.

27.Valutazione di impatto sulla protezione dei dati

1.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 – previa consultazione con il Responsabile della Protezione dei Dati - all'effettuazione di una valutazione di impatto sulla protezione dei dati personali.

2.Il Titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

3.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.

28.Utilizzo in ambienti di lavoro

1.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'Ente, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

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

3.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

29.Sistemi integrati di trattamento dei dati

1.In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, previo accordo scritto con gli Organi interessati, è possibile il ricorso a sistemi integrati di trattamento dei dati tra diversi soggetti, pubblici e privati.

2.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.

3.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.

4.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.

30.Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

1.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 e dagli artt. 37 e ss. del D. lgs. 51/2018 relativo 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.

31.Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali

1.Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal Titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82 del RGPD.

2.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.

3.Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2 del RGPD.

32.Provvedimenti attuativi

1.Compete al Presidente della Provincia 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 e la definizione di ogni ulteriore e specifico elemento ritenuto utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento e dalle leggi ivi applicabili, ed entro i limiti da questi ultimi imposti.

2.Specifici disciplinari potranno essere redatti di concerto tra Il Presidente della Provincia e il Supervisore al fine di regolare nello specifico determinati trattamenti inerenti il sistema di videosorveglianza.

3.Previa istanza da parte del Supervisore, nonché in ottemperanza ed entro i limiti, il contesto, le finalità e le modalità di quanto disposto dal presente Regolamento e dalle leggi ivi applicabili, spetterà altresì al Presidente della Provincia la scelta di adottare nuovi strumenti, sistemi e tecnologie integrativi all'attuale sistema di videosorveglianza.

4.Il Presidente della Provincia dovrà specificare, per ogni nuova soluzione adottata:

- l'individuazione dei soggetti inquadrati nell'organigramma dell'ente che svolgeranno il ruolo di supervisor;
- le finalità del trattamento;
- le motivazioni dell'installazione dell'impianto;
- la sintetica descrizione del trattamento e del flusso informativo;
- l'architettura tecnologica generale dei sistemi di gestione dei dati;
- l'eventuale necessità di effettuare una valutazione di impatto sulla protezione dei dati;
- 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.

5.Il Presidente della Provincia provvederà ad aggiornare le informazioni con apposito provvedimento di organizzazione ogni qualvolta un trattamento subisca variazioni rilevanti.

6.In seguito all'adozione di nuove soluzioni tecnologiche, rimane sempre in capo ai Supervisor i l'onere di adottare 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 e la lista relativa al loro aggiornamento;
- 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'attuazione di tutte le misure che garantiscano la sicurezza dei dati trattati e dei sistemi implementati.
- l'aggiornamento delle informative e della cartellonistica.

7. Sarà sempre onere del Supervisore valutare le idonee garanzie e competenze offerte da tutti i fornitori coinvolti, nonché di chiedere alle ditte produttrici le specifiche delle tecnologie e dei sistemi utilizzati, ivi comprese le misure di sicurezza, che verranno individuate con apposita documentazione tecnica rilasciata dalla medesima Ditta produttrice, da conservare unitamente ai disciplinari adottati.

8. La Ditta produttrice dovrà fornire altresì le caratteristiche fisiche degli strumenti e la descrizione del loro funzionamento.

9. Le scelte implementative del Supervisore, effettuate sulla base degli indirizzi forniti dal Presidente della Provincia, dovranno sempre avere il fine di ridurre al minimo i rischi di violazione dei dati, ed in particolare di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati personali.

33. Modifiche regolamentari

1. 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. In ogni caso ogni modifica al presente Regolamento dovrà essere approvata da parte del Consiglio Provinciale.

34. Entrata in vigore e norme di rinvio

1. Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.

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

3. Per quanto non disciplinato dal presente Regolamento si rinvia al Codice della Privacy come modificato dal D. lgs 101/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, al Regolamento UE 2016/679 e al D. lgs 51/2018 relativo 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 ai provvedimenti generali sulla videosorveglianza approvati dall'Autorità garante per la protezione dei dati personali e alle indicazioni centrali dell'Anci, UPI e del Ministero d