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

Approvato con deliberazione del Consiglio comunale n. 20 del 6 giugno 2023
(in vigore dal 6 giugno 2023)

Sommario

CAPO I – DISPOSIZIONI GENERALI

1. Oggetto del Regolamento
2. Definizioni
3. Norme di riferimento
4. Ambito di applicazione
5. Principi generali
6. Finalità del trattamento

CAPO II – MODALITA' DI TRATTAMENTO DEI DATI

7. Acquisizione dei dati
8. Trattamento da parte degli operatori
9. Utilizzo di particolari sistemi mobili
10. Accesso ai dati
11. Comunicazione a terzi
12. Conservazione dei dati
13. Cessazione del trattamento
14. Limitazione del trattamento

CAPO III – SOGGETTI COINVOLTI NEI TRATTAMENTI

15. Titolare del trattamento
16. Supervisore del trattamento
17. Soggetti autorizzati al trattamento dei dati personali
18. Soggetti esterni che trattano dati per conto del Titolare
19. Amministratori di Sistema

CAPO IV – MISURE DI SICUREZZA

20. Accesso fisico ai sistemi e ai luoghi
21. Accesso logico ai sistemi e ai dati
22. Sicurezza nelle trasmissioni
23. Utilizzo degli strumenti e dei supporti di memorizzazione

CAPO V – OBBLIGHI DEL TITOLARE

24. Informativa
25. Diritti dell'interessato
26. Valutazione di impatto sulla protezione dei dati
27. Utilizzo in ambienti di lavoro

CAPO VI – ALTRE DISPOSIZIONI

28. Sistemi integrati di trattamento dei dati

29. Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale
30. Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali
31. Provvedimenti attuativi
32. Modifiche regolamentari
33. Norma di rinvio
34. Entrata in vigore

CAPO I – DISPOSIZIONI GENERALI

1. Oggetto del Regolamento

1. 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 Seriate 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.
2. 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

1. Ai fini del presente Regolamento si intende:
   - **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.
   - **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.
   - **Codice:** è il D. Lgs. 196/2003, "Codice in materia di protezione dei dati personali".
   - **RGPD**: acronimo di "Regolamento Generale di Protezione del 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".
   - **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 Seriate.
   - **Contitolari del trattamento**: ai sensi dell'art 17 del D.Lgs n. 51/2018: sono due o più titolari del trattamento che determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, nonché le relative responsabilità.
   - **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 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", e s.m.i.;
- D.P.R. 22 giugno 1999, n. 127 in materia di impianti per la rilevazione degli accessi di veicoli ai centri storici ed alle zone a traffico limitato;
- D. Lgs 51/2018: 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.

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 ed alle eventuali informazioni sulla geolocalizzazione geografica, svolti sotto la diretta titolarità del Comune di Seriate e/o da altri soggetti in contitolarità con il Titolare, all'interno del territorio del Comune di Seriate e degli altri Enti con esso, eventualmente, convenzionati.

5. Principi generali

1. Il trattamento dei dati avviene mediante acquisizione degli stessi dal sistema di videosorveglianza del Comune di Seriate, collegato alla centrale di controllo ubicata presso la sede del Corpo di Polizia Locale ed, eventualmente, a quelle di altri Comandi di Polizia Locale e/o Forze di Polizia in funzione degli accordi sottoscritti con la Città di Seriate;
2. Il trattamento di acquisizione immagini, videoriprese e informazioni sulla eventuale 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 l'acquisizione di dati anonimi od opportune tramite 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 siano incompatibili con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana.

6. Finalità del trattamento

1. Le finalità di utilizzo degli impianti di videosorveglianza di cui al presente regolamento sono conformi alle funzioni istituzionali attribuite al Comune di Seriate dalla legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Municipale, dalle conseguenti Leggi Regionali in materia di ordinamento della Polizia Municipale, dallo statuto e dai regolamenti comunali, nonché dal decreto legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 e s.m.i. *"Disposizioni urgenti in materia di sicurezza delle città"*.
2. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre Polizie Locali e delle Forze di Polizia a competenza generale, dovrà essere specificamente disciplinato con appositi atti o protocolli operativi condivisi.
3. L'utilizzo degli impianti di gestione e acquisizione di immagini, videoriprese e dati di geolocalizzazione è finalizzato a:
   a) prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'art. 4 del Decreto Legge n.14/2017 e delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art.50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del D.Lgs. 267/2000;
   b) tutela della sicurezza urbana e della sicurezza pubblica in ambito comunale nei limiti delle attribuzioni conferite ai rispettivi soggetti utilizzatori dei dati;
   c) vigilanza sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;

d) tutela della protezione civile e della salute;
e) tutela della sicurezza stradale, monitoraggio dei flussi di traffico anche attraverso rilevazioni di tipo quantitativo e statistico, consentendo, altresì ove possibile, la ricostruzione dinamica dei sinistri stradali;
f) tutela ambientale e polizia amministrativa;
g) tutela dell'ordine, del decoro e della quiete pubblica;
h) unicamente ai soggetti titolari delle funzioni di polizia giudiziaria, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, acquisizione di prove, nell'ambito di attività di P.G.; In oltre il sistema è finalizzato:
i) alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze attribuite dalla legge;
j) al controllo di aree specifiche del territorio qualora si renda necessario ed in occasione di eventi a rilevante partecipazione di pubblico;
k) al perseguimento degli obiettivi organizzativi e di coordinamento degli interventi e delle risorse;
l) alla prevenzione, all'accertamento ed alla repressione di comportamenti illeciti derivanti dall'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose, oltre che al monitoraggio per il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti.
m) per i soggetti fermati o in stato di arresto trattenuti presso idonea camera di sicurezza e monitorati tramite impianto di videosorveglianza. Il soggetto detenuto verrà informato tramite apposita segnaletica della sua sottoposizione a videoripresa. Dovranno essere attuate tutte le misure atte a garantire la proporzionalità del trattamento. Le immagini saranno conservate per un periodo massimo di 72 ore salvo comprovate esigenze di carattere giudiziario o per motivi di pubblica sicurezza.

4. Nel caso in cui soggetti privati intendano realizzare impianti di videosorveglianza che riprendono strade o luoghi pubblici o ad uso pubblico il Titolare può assumere, previa verifica di idoneità degli impianti, la gestione dello stesso. I privati interessati assumono gli oneri relativi all'installazione dell'impianto e la connessione con il sistema del Comune di Seriate, il rispetto delle prescrizioni normative in materia, la conformità alle caratteristiche tecniche dell'impianto pubblico e le mettono a disposizione dell'ente a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa. Questi aspetti dovranno essere regolamentati attraverso una apposita convenzione sottoscritta tra le parti.
5. Il sistema di videosorveglianza può comportare il trattamento di dati personali che possono essere rilevati da telecamere tradizionali eventualmente munite di algoritmi di analisi video, metadatazione, o varchi lettura targhe connessi a black list o altre banche dati, in grado di verificare in tempo reale i dati e/o la regolarità di un transito di un veicolo, in conformità alla DPIA.
6. Il Comune di Seriate promuove e attua, per la parte di competenza, politiche di controllo del territorio e dei veicoli in transito lungo i principali assi stradali di collegamento eventualmente in collaborazione con altri Organi di Polizia o Enti terzi, sulla base di accordi, convenzioni e protocolli operativi; ciascun Ente manterrà la piena responsabilità dei dati personali trattati.
7. Nel rispetto delle finalità previste nel presente regolamento, dalle immagini di videosorveglianza potranno essere acquisiti elementi strettamente necessari alla verbalizzazione di violazioni amministrative, nel rispetto del principio di minimizzazione ex art. 5 RGPD e delle vigenti normative e regolamenti.
8. Il sistema di videosorveglianza in uso presso il Corpo di Polizia Locale di Seriate consente l'utilizzo dell'impianto in modalità condivisa con altre Polizie Locali e/o le Forze di Polizia Statali al fine di rendere il sistema strumento di prevenzione e di razionalizzazione dell'azione di polizia su tutto il territorio. Nel rispetto delle finalità previste dal presente Regolamento, l'Ente potrà promuovere politiche di controllo del territorio integrate con organi istituzionalmente preposti alla tutela della sicurezza e dell'ordine pubblico. Dette politiche di controllo integrato e/o di collaborazione con altri

Corpi o Organi preposti alla tutela della sicurezza e dell'ordine pubblico, anche al fine di consentire la visualizzazione diretta delle immagini degli apparati di videosorveglianza, vengono previamente disciplinati con separati accordi in forma scritta disciplinanti l'utilizzo condiviso del sistema comunale di videosorveglianza nonché le modalità di acquisizione e trattamento dei dati da parte di terzi soggetti autorizzati.

9. Ai sensi di quanto previsto dall'art.4 della Legge 20 maggio 1970, n.300 e s.m.i., gli impianti di videosorveglianza non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati. Nel caso in cui il Titolare intenda installare delle videocamere all'interno di edifici pubblici o in luoghi quali piazzole ecologiche (per la tutela del patrimonio e la prevenzione di reati) che possono riprendere anche occasionalmente dei lavoratori si dovrà procedere alla relativa regolamentazione dell'impianto attraverso:
   a) condivisione delle finalità e della predisposizione dell'impianto con le rappresentanze sindacali
   b) in caso di assenza delle rappresentanze sindacali comunicazione all'ispettorato provinciale del lavoro
   c) segnaletica nei locali video sorvegliati
   d) informativa da trasmettere ai lavoratori

CAPO II – MODALITA' DI TRATTAMENTO DEI DATI

7. 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 nei siti individuati dalla Giunta Comunale in funzione delle finalità del predetto regolamento.
3. Il Supervisore competente definisce il numero e la tipologia degli apparati di geolocalizzazione, eventualmente in dotazione al Corpo di Polizia Locale, utilizzati in conformità con la propria autonomia organizzativa e competenza.
4. Per quanto concerne il sistema di videosorveglianza territoriale, facente capo alla Polizia Locale, la diretta visione delle immagini nelle sale o centrali operative è limitata ad obiettivi particolarmente sensibili e strategici per la sicurezza urbana o in presenza del requisito di pubblico interesse nel rispetto dei criteri di necessità, pertinenza, non eccedenza dei dati o dei trattamenti.

8.Trattamento da parte degli operatori

1. Nell'ambito dell'Amministrazione comunale è designato "Supervisore" del trattamento dei dati rilevati con apparecchi di videosorveglianza il Dirigente - Comandante del Corpo di Polizia Locale, per quanto concerne le apparecchiature collegate alla centrale operativa del Comando di Polizia Locale e nella disponibilità operativa del Corpo di Polizia Locale impiegate per le funzioni ad esso attribuite.
2. Il Titolare del trattamento può designare "Supervisori" ulteriori Dirigenti facenti parte dell'Ente, relativamente ai dati acquisiti con le apparecchiature nella disponibilità dei rispettivi settori in ragione delle materie di competenza.
3. Tali designati vengono puntualmente individuati con atto del "Titolare", in relazione al trattamento delle immagini di propria competenza così come definito nei commi 1 e 2 del presente articolo, con cui impartire direttive e fornire indicazioni per la gestione ottimale della videosorveglianza. Possono

essere individuati dal Comune per il proprio ambito di competenza ulteriori designati in ragione di ulteriori necessità.

4. I "Supervisori" individuano e nominano, con proprio provvedimento, gli autorizzati alla gestione dell'impianto nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio e con specifici limiti di azione.
5. I dati acquisiti sono trattati, nel rispetto delle misure minime indicate dalla normativa relativa alla protezione delle persone fisiche, da soggetti per cui sono stati definiti specifici profili di accesso.
6. 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. Utilizzo di particolari sistemi mobili.

1. Il sistema di videosorveglianza in uso al Comando di Polizia Locale di Seriate comprende apparecchi mobili, quali:

   - body cam e dash cam;

   - fototrappole e sistemi mobili di videosorveglianza.

2. Gli operatori di Polizia Locale possono essere dotati, nello svolgimento di servizi operativi e di controllo del territorio, delle Body Cam (ossia sistemi di ripresa indossabili) e delle Dash Cam (telecamere installate a bordo veicoli di servizio) in conformità delle indicazioni dettate dal Garante della Privacy con nota 26 luglio 2016, prot. n. 49612, con cui sono state impartite le prescrizioni generali di utilizzo dei predetti dispositivi il cui trattamento dei dati è ricondotto nell'ambito del D.lgs 51/2018 trattandosi di "*dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela all'ordine e della sicurezza pubblica, nonché di polizia giudiziaria*". Il Comandante del Corpo curerà la predisposizione di uno specifico disciplinare tecnico interno, da somministrare agli operatori di Polizia Locale che saranno dotati delle apparecchiature, con specificazione dei casi in cui queste devono essere attivate, dei soggetti autorizzati a disporre l'attivazione, delle operazioni autorizzate nel caso di emergenza e di ogni altra misura organizzativa e tecnologica necessaria alla corretta e legittima gestione dei dispositivi e dei dati trattati.
3. Il Corpo di Polizia Locale può dotarsi di telecamere riposizionabili, anche del tipo foto-trappola, con generazione di allarmi da remoto per il monitoraggio attivo. Le modalità di impiego dei dispositivi in questione saranno disciplinate con apposito provvedimento del Comandante del Corpo di Polizia Locale.
4. Gli apparati di videosorveglianza modulare riposizionabili vengono installati secondo necessità, nei luoghi teatro di illeciti penali; possono essere utilizzati per accertare illeciti amministrativi, solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine. Qualora non sussistano finalità di sicurezza o necessità di indagine previste dal D.lgs 51/2018 che esimono il Titolare dall'obbligo di informazione, si provvederà alla previa collocazione della adeguata cartellonistica informativa agli utenti frequentatori di dette aree.
5. Il Corpo di Polizia Locale, per lo svolgimento delle attività di competenza può dotarsi di ogni altra tecnologia di ripresa video e di captazione di immagini necessaria al raggiungimento delle finalità istituzionali. In particolare può dotarsi di Sistemi Aeromobili a Pilotaggio Remoto – droni – sia per l'esecuzione di riprese ai fini di tutela della sicurezza urbana, sia per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. In ogni caso, i dispositivi e il loro utilizzo devono essere conformi alla normativa vigente, con particolare riferimento alla regolamentazione adottata dall'Ente Nazionale per l'Aviazione Civile e al Codice della Navigazione. Le modalità di impiego dei dispositivi in questione saranno disciplinate con apposito provvedimento del Comandante di Polizia Locale.
6. Il trattamento dei dati personali effettuati con simili sistemi di ripresa deve rispettare i principi di cui all'art. 11 del Codice ed in particolare i dati personali oggetto di trattamento debbono 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.

10. Accesso ai dati.

1. Ogni richiesta di accesso dovrà essere specifica, formulata per iscritto, motivata ed indirizzata al Supervisore del trattamento dei dati competente ordinariamente entro tre (3) giorni dall'accadimento dei fatti oggetto di interesse. L'estrazione dei dati sarà effettuata compatibilmente con la disponibilità di personale da impiegare; qualora le istanze pervengano tardivamente o, in ragione della disponibilità di personale da impiegare, non possano essere evase entro i termini di conservazione dei dati fissati dal presente regolamento, il Titolare, il Supervisore ed il Responsabile del trattamento sono esonerati dalla responsabilità relativa al mancato rilascio dei dati richiesti.
2. Per finalità di indagine, l'autorità giudiziaria e la polizia giudiziaria possono richiedere ed acquisire copia delle immagini in formato digitale.
3. Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, copia delle riprese in formato digitale può essere richiesta ed acquisita dall'organo di polizia stradale che ha proceduto ai rilievi ed in capo al quale è l'istruttoria relativa all'incidente.
4. Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'art. 391-quater c.p.p., può richiedere ed acquisire copia delle riprese in formato digitale previo pagamento delle relative spese individuate con apposita deliberazione di giunta comunale sulle tariffe di accesso ai documenti amministrativi.
5. Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al supervisore del trattamento, secondo quanto stabilito dal comma 1 del presente articolo, che i filmati siano conservati oltre i termini di legge, per essere messi a disposizione dell'organo di polizia procedente. Spetta all'organo di polizia procedente presentare richiesta di acquisizione dei filmati. Tale richiesta deve pervenire entro tre mesi dalla data dell'evento, decorsi i quali i dati non saranno ulteriormente conservati.
6. In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal supervisore del trattamento dei dati deve annotare le operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, con lo scopo di garantire la genuinità dei dati stessi.

11. 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. I sistemi di gestione potranno essere utilizzati anche a supporto di indagini dell'Autorità Giudiziaria, di organi di Polizia o di Polizia Locale.
3. Gli organi di Polizia e l'Autorità Giudiziaria, qualora non sia possibile l'accesso diretto ai dati regolamentato da apposito accordo o convenzione con il titolare del trattamento, potranno accedere alle informazioni raccolte tramite consultazione presso le sedi del Titolare, trasmissione telematica o consegna di copia su supporto digitale o analogico. L'estrazione dei dati sarà effettuata compatibilmente con la disponibilità di personale da impiegare; qualora le istanze pervengano tardivamente o, in ragione della disponibilità di personale da impiegare, non possano essere evase entro i termini di conservazione dei dati fissati dal presente regolamento, il Titolare e il Supervisore sono esonerati dalla responsabilità relativa al mancato rilascio dei dati richiesti.

12. Conservazione dei dati

1. I dati personali oggetto di trattamento effettuato con l'utilizzo degli impianti di videosorveglianza nel rispetto delle misure minime indicate dalla normativa relativa alla protezione delle persone fisiche sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per le finalità di cui all'articolo 6 del presente regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;

c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;

d) conservati per un periodo di tempo non superiore a sette (7) giorni dalla data della rilevazione, fatte salve le esigenze di ulteriore conservazione di seguito indicate:

   I. esigenze di indagine e di prevenzione dei reati svolte dalla Polizia Giudiziaria autonomamente o su indicazione dell'Autorità Giudiziaria;

   II. a seguito di ordine di sequestro o richiesta di messa a disposizione emanato dall'Autorità Giudiziaria;

   III. esigenze di pubblica sicurezza a seguito di specifica richiesta dell'Autorità prefettizia o di Polizia;

   IV. a seguito di rilevazione di fatti costituenti reato;

   V. esigenze di accertamento di illeciti di natura amministrativa; i dati saranno conservati in funzione della durata del procedimento sanzionatorio, comprensivo dei termini conseguenti alle eventuali opposizioni / ricorsi;

   VI. nel caso di acquisizione dei dati di geolocalizzazione i tempi di conservazione, comunque non superiori a trenta (30) giorni, saranno predeterminati a seconda delle necessità di carattere organizzativo che hanno motivato l'utilizzo di tali strumenti, 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;

   Nei casi disciplinati dai punti da I a VI dovrà essere informato il Supervisore competente, che darà esplicite disposizioni ai soggetti designati di operare per tale fine.

2. 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.

13. 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;

14. Limitazione del trattamento

1. L'interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'art. 18 del RGPD e all'art.14 del D.Lgs. 51/2018.
2. 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

15. Titolare del trattamento

1. Il Comune di Seriate 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.
2. 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, dell'art. 23 del D.Lgs.51/2018, ed eventualmente la consultazione preventiva al Garante per la protezione dei dati personali di cui all'art. 36 RGPD e dell'art. 24 del D.Lgs.51/2018, 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 Supervisori 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.

16. Supervisori del trattamento

1. Il Titolare del trattamento designa quali Supervisore del trattamento di dati personali effettuato mediante l'utilizzo degli impianti di cui al presente regolamento:
   - il Comandante del Corpo di Polizia Locale del Comune di Seriate, per quanto di competenza relativamente ai sistemi di videosorveglianza posti a dotazione del Corpo di Polizia Locale,
   - i dirigenti degli altri servizi facenti parte dell'Amministrazione comunale, relativamente agli eventuali dati acquisiti con le apparecchiature nella disponibilità dei rispettivi settori in ragione delle materie di competenza.

La nomina è effettuata con atto del Sindaco, nel quale sono analiticamente specificati i compiti affidati. In particolare il Supervisore:

   a) individua i siti in cui potranno essere collocati i sistemi di acquisizione delle immagini, sulla base delle necessità rilevate, delle finalità previste dal presente regolamento ed in osservanza al principio di proporzionalità del trattamento, proponendo alla Giunta comunale l'approvazione del relativo elenco;
   b) 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;
   c) 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;

d) 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;
e) provvede a rendere disponibile l'informativa "minima" agli interessati;
f) 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;
g) assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
h) 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 e dell'art.25 del D.Lgs.51/2018;
i) 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;
j) 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;
k) assiste il Titolare nel garantire 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 e degli artt. 26 e 27 del D.Lgs. 51/2018;
n) supporta il Titolare, unitamente al Responsabile della Protezione dei Dati, nell'effettuazione della valutazione di impatto sulla protezione dei dati e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali;
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 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.

2. I Supervisori, 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.

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

17. 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;
   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.

18. 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 o della rete di trasmissione, 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.

19. Amministratori di Sistema e di Rete

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 e/o della rete di trasmissione dei dati, assegnando con precisa definizione i rispettivi perimetri operativi e le responsabilità.
3. Coloro che svolgono mansioni di cui ai commi precedenti 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 e/o della rete di trasmissione dei dati. Nel caso di nomina di personale esterno all'Ente, questi ultimi, a loro volta, sono tenuti a mantenere aggiornato l'elenco delle persone fisiche che operano sul sistema e sulla rete per conto del Titolare, rendendolo disponibile su richiesta dell'Ente.
5. Il Supervisore ed i responsabili sono tenuti, per i contesti di loro competenza e responsabilità, al rispetto delle prescrizioni specificate nel provvedimento del Garante Privacy sugli "amministratori" e negli aggiornamenti successivi.

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 zone ad accesso riservato.
2. Nel caso in cui il trattamento venga effettuato presso locali interni all'Ente, l'accesso a questi ultimi nel corso del trattamento 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 all'autorizzazione da parte del Titolare o del Supervisore. 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. Nel caso in cui 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 alle immagini ed ai dati è consentito esclusivamente:
   a) al Titolare, al Supervisore ed ai soggetti autorizzati al trattamento;
   b) alla Polizia Locale o altre Forze di Polizia, sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente o sulla base di accordi / convenzioni preventivamente stipulati con il titolare del trattamento, nonché per finalità di indagine dell'Autorità Giudiziaria sulla base di formale richiesta 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 e/o della rete specificamente designati per tale contesto e preventivamente autorizzati al trattamento dei dati.
3. 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.

22. Sicurezza nelle trasmissioni

1. 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.
2. I Supervisori 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.

23. 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 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 non consentito in alcun modo il recupero dei dati trattati.

CAPO V – OBBLIGHI DEL TITOLARE

24. Informativa

1. I soggetti interessati che stanno per accedere o che si trovano in una zona videosorvegliata, devono essere sempre informati mediante appositi cartelli, nei casi specificatamente previsti dalla normativa vigente. A tal fine il Titolare utilizzerà una informativa cosiddetta di "primo" e di "secondo" livello. 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. Il cartello è posizionato prima dell'accesso nell'area monitorata. Detto cartello riporterà le informazioni più importanti, comprese quelle di maggior impatto per l'interessato (es. finalità del trattamento, dati del Titolare, i dati di contatto del Responsabile della Protezione dei Dati e i diritti degli interessati, il periodo di conservazione)
2. Verrà inoltre riportato anche il luogo ove l'interessato potrà prendere visione dell'informativa per esteso, cosiddetta di "secondo livello". Quest'ultima 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.
3. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, possono essere installati più cartelli. 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.
4. L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo e di polizia giudiziaria.

5. 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.

25. Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, compatibilmente con i fini investigativi a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati di cui al D.lgs.51/2018, ha diritto previa presentazione di apposita istanza:

   a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;

   b) di essere informato sugli estremi identificativi del Titolare del trattamento, oltre che 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 ed in generale di tutto quanto previsto ex art. 13 RGPD e art. 10 e ss. D. lgs 51/2018;

   c) di ottenere:

   - la conferma dell'esistenza o meno di dati personali che lo riguardano;
   - la cancellazione nei casi previsti dal Regolamento UE 2016/679 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 nei casi previsti dal Regolamento UE 2016/679, 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. Il designato informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti;

   e) 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;

2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al titolare o al designato al trattamento dati a norma dell'art.10 del presente regolamento. È considerata sempre l'opportunità di coinvolgere il Responsabile della Protezione Dati.

26. Valutazione di impatto sulla protezione dei dati

1. In ossequio al disposto di cui all'art. 35 RGPD, e dell'art 23 del D.Lgs 51-2018 qualora il trattamento di dati realizzato mediante i sistemi oggetto del presente regolamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare provvederà, previa consultazione del Responsabile della Protezione dei Dati, all'effettuazione di una valutazione di impatto sulla protezione dei dati personali. Il Titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento potrebbe rappresentare un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
2. 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

1. Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970, n. 300 e s.m.i, 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.
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

28. Sistemi integrati di trattamento dei dati

1. 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.
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;
   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;
   c) collegamento del sistema di videosorveglianza con la sala operativa degli organi di polizia.

3. Le modalità di trattamento sopra elencate richiedono, oltre ad una convenzione scritta tra i titolari interessati, l'adozione di specifiche misure di sicurezza, quali:
   a) la nomina degli autorizzati ad accedere ai dati, sistemi di autenticazione e l'adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi.

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 e dell'art. 23 del D.Lgs. 51/2018.

29. 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.

2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati personali, così come individuato dal precedente art. 8.

30. 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, il designato e/o il responsabile del trattamento sono esonerati dalla responsabilità se dimostrano 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.

31. Provvedimenti attuativi

1. Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi conseguenti al presente Regolamento, nonché la definizione di ogni ulteriore e specifica disposizione o elemento ritenuto utile, in coerenza con gli indirizzi stabiliti dal presente regolamento, che a titolo esemplificativo e non esaustivo si identificano in quelle seguito riportate:
   - le finalità del trattamento;
   - le motivazioni dell'installazione dell'impianto o dell'attivazione di nuove forme di videosorveglianza;
   - l'approvazione dell'elenco dei siti in cui verranno installati in modo permanente i sistemi di acquisizione delle immagini, sulla base delle necessità e motivazioni indicate dal Supervisore; fanno eccezione gli impianti ed i sistemi di acquisizione dati ed immagini mobili di cui all'art. 9 del presente Regolamento nell'esclusiva disponibilità del Comando di Polizia Locale.
   - le categorie di destinatari ai sensi dell'art. 28 del presente regolamento (sistemi integrati di videosorveglianza) a cui vengono resi disponibili i dati.
2. La Giunta Comunale con apposito provvedimento attuativo o propositivo provvederà ad aggiornare quanto attribuito alla propria competenza dal presente articolo ogni qualvolta un trattamento subisca variazioni rilevanti.
3. Spetta invece ai Supervisori, con atto proprio, provvedere a quanto previsto dall'art. 16 del presente regolamento.

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. Norma di rinvio

Per tutto quanto non disciplinato dal presente Regolamento si fa rinvio alle Leggi vigenti, ai provvedimenti attuativi delle medesime, alle decisioni del Garante e ad ogni altra normativa, speciale, generale, nazionale e comunitaria in materia di protezione e trattamento dei dati personali nell'ambito della videosorveglianza.

34. Entrata in vigore

1. Il presente regolamento entra in vigore il decimo giorno successivo alla sua pubblicazione all'Albo Pretorio, salvo non sia stata dichiarata immediatamente eseguibile la delibera di approvazione ai sensi dell'art. 134 del D.Lgs. 267/2000.
2. Il presente Regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.