COMUNE DI COMO

REGOLAMENTO

PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO TRAMITE DISPOSITIVI DI ACQUISIZIONE IMMAGINI, REGISTRAZIONE, CONSERVAZIONE E GESTIONE DI IMMAGINI, AUDIO-IMMAGINI, VIDEORIPRESE.

Approvato con deliberazione del Consiglio comunale n. 43 del 22/11/2021

Sommario

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, dal Comune di Como.
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 e in conformità alle norme e linee guida elencate al successivo art. 3 e ss.mm.ii..

In particolare, il presente Regolamento:

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

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:

a) 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.
b) 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".
c) 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 Comune di Como (di seguito anche semplicemente "Ente").
d) Responsabile del trattamento è una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che tratta dati personali per conto del titolare del trattamento ai sensi delle linee guida 7/2020 European data protection board.
e) Autorizzato al trattamento: è la persona fisica, designato dal Titolare, autorizzato sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.
f) Responsabile della Protezione dei Dati: è una figura prevista dall'art. 37 del RGPD. 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. Coopera 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 e degli artt. 28. 29 e 30 del d.lgs. 51/2018).

g) Interessato: la persona fisica cui si riferiscono i dati personali oggetto di trattamento.

2) Ai fini delle definizioni di cui al presente Regolamento si deve fare riferimento all'art. 4 del RGPD 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:

a) 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";

b) Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali";

c) 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";

d) D.L. n. 14/2017 *<<Disposizioni urgenti in materia di sicurezza delle città>>,* convertito nella L. n. 48/2017;

e) D.L. n. 11/2009, (c.d. Decreto Maroni) convertito nella L. n. 38/2009, che all'art. 6, commi 7 e 8, stabilisce che «*7. Per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico. 8. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione*»;

f) 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";

g) 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;

h) 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;

i) Legge 20 maggio 1970, n. 300;

j) 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 e videoriprese, 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 precedentemente definito si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 del RGDP e, in particolare:

a) 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.

b) 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.

c) 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 è stata effettuata dall'Ente su tutto il territorio comunale e che gli impianti di videosorveglianza, laddove previsti, sono stati adottati in quanto 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).

d) 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. È consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana.

6. Finalità del trattamento e base giuridica

1) Il trattamento 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.
2) Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:
    a) tutela della sicurezza urbana nei luoghi pubblici o aperti al pubblico;
    b) tutela della sicurezza stradale, per monitorare la circolazione lungo le strade del territorio comunale e rilevare le infrazioni nonché fornire ausilio in materia di polizia amministrativa in generale;
    c) tutela del patrimonio comunale, per presidiare gli accessi agli edifici comunali, dall'interno o dall'esterno, e le aree adiacenti o pertinenti ad uffici od immobili comunali;
    d) tutela ambientale e rilevazione infrazioni;
    e) all'esigenza, unicamente in qualità di polizia giudiziaria, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali a norma del D. Lgs. 51/2018.
3) 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 Forze di Polizia e/o sicurezza, dovrà essere specificamente disciplinato con appositi accordi di contitolarità, patti per l'attuazione della sicurezza urbana, ecc. secondo la vigente normativa.
4) A tal riguardo l'Ente potrà altresì 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.

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 in siti predefiniti dal Titolare del Trattamento competente e tramite specifico atto di determinazione.
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.

4) Utilizzo di particolari sistemi mobili (es. dashcam, fototrappole, bodycam, ecc.) sono disciplinati secondo apposito disciplinare tecnico e/o provvedimento di assegnazione del Dirigente competente previa idonea valutazione di impatto sulla protezione dei dati.

8. 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:
   a) Visione delle immagini e delle videoriprese acquisite in tempo reale;
   b) Consultazione dei dati registrati;
   c) Gestione dei dati acquisiti, tra cui cancellazione, estrazione di copia su supporti digitali e/o stampa su supporti analogici;
   d) 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.

4) Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità ai sensi dell'art. 30 del GDPR.

9. Estrazione di copia

1) È 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.

10. 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 Titolare

del trattamento, ovvero l'incaricato designato, 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 delle Forze di Polizia 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 Titolare del Trattamento sottoscritta dal richiedente e previa identificazione.
5) Ogni attività effettuata deve essere tracciata.
6) Nel caso in cui il trattamento dei dati personali sia effettuato per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, ovvero a tutela della pubblica sicurezza da minacce che la potrebbero pregiudicare, la disciplina di accesso ai dati è regolata dall'art. 11 del D.Lgs. 51/2018, ovvero quella della registrazione di cui dall'art. 21 del medesimo decreto

11. Conservazione dei dati

1) I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione, salvo diverse esigenze che impongano un termine più lungo di conservazione, documentate caso per caso e rispondenti alle finalità istituzionali perseguite dall'Ente. Decorso il periodo di conservazione prestabilito, i dati registrati sono cancellati con modalità specificamente determinate a seconda del sistema di videosorveglianza.
2) 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 titolare del trattamento, che darà esplicite disposizioni ai soggetti designati ad operare per tale fine.

12.Cessazione del trattamento

1) In caso di cessazione, per qualsiasi causa, di un trattamento di dati personali, gli stessi possono essere:

a) distrutti;

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

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

2) La cessazione del trattamento dei dati in ogni caso è conforme alle disposizioni del RGPD, ovvero dell'articolo 14 del d. lgs. 51/2018.

13.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 all'art. 59 del D.Lgs. n. 196/03.
2) Ogni richiesta dovrà essere indirizzata al Titolare del Trattamento, ovvero all'incaricato designato.
3) 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.
4) 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 titolare del trattamento. In tal caso il difensore potrà presentare la richiesta motivata. Salvo l'ipotesi di conservazione per diverse finalità, i dati si intendono disponibili per i normali tempi di conservazione.
5) Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al Titolare del trattamento, ovvero all'incaricato designato, 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.
6) In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal Titolare del trattamento dovrà tenere traccia delle operazioni eseguite.

CAPO III – SOGGETTI COINVOLTI NEI TRATTAMENTI

14.Titolare del trattamento

1) L'Ente 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 pro tempore, dal dirigente dell'area presso il quale l'impianto o dispositivo è assegnato a seconda della struttura organizzativa, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.
2) Il dirigente in qualità di Designato al trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti per quota parte e, fatta salva ogni altra attribuzioni del Sindaco:

a) definisce le linee organizzative per l'applicazione della normativa di settore, confrontandosi direttamente con il Responsabile della Protezione dei Dati o interpellandolo per le questioni di competenza di quest'ultimo;

b) dispone le eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;

c) dispone quando necessario la valutazione di impatto sulla protezione dei dati di cui all'art. 35 del RGPD ed eventualmente la consultazione preventiva al Garante per la protezione dei dati personali di cui all'art. 36 RGPD, oltre a qualsiasi altra consultazione ritenuta necessaria per il corretto trattamento dei dati, interagendo con l'autorità nei casi previsti dalla norma;

d) designa i soggetti autorizzati come definiti all'art. 2, lettera d);

e) detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti;

f) vigila sulla puntuale osservanza delle disposizioni impartite.

15. Soggetti autorizzati al trattamento dei dati personali

1) Il Titolare 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 Titolare del trattamento;

f) segnalare al Titolare del Trattamento 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 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 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.

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.

16. Soggetti esterni che trattano dati per conto del Titolare

1) Il Titolare del trattamento ha la facoltà di avvalersi di soggetti esterni, in qualità di responsabili e/o autorizzati al trattamento, 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.
5) Il Titolare del Trattamento aggiorna periodicamente la lista dei responsabili esterni del trattamento.

17. Responsabili ed autorizzati al trattamento

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

CAPO IV – MISURE DI SICUREZZA

18. 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) In caso di locali interni all'Ente l'accesso è consentito esclusivamente al Titolare, ai soggetti autorizzati e ai responsabili, individuati ai sensi degli articoli 16 e 17 del presente Regolamento. L'accesso da parte di soggetti diversi da quelli precedentemente indicati è subordinato al rilascio, da parte del Titolare, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. 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) 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.

19. 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 Titolare 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 del trattamento 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) ai soggetti legittimati ai sensi del presente regolamento;

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.

4) L'accesso agli impianti di videosorveglianza di cui al presente regolamento avviene esclusivamente da postazioni dedicate situate nella control room del Comando della Polizia Locale del Comune di Como ed in quella del Settore Innovazione Tecnologica, ovvero l'accesso ai dati può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide, strettamente personali, e di vari livelli di sicurezza rilasciate dall'Amministratore di sistema.
5) L'accesso agli impianti di videosorveglianza è consentito esclusivamente al Titolare del trattamento comunale ed agli incaricati, individuati ai sensi del presente Regolamento.

20. 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) 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 – DIRITTI DEGLI INTERESSATI

21. Informativa

1) Gli interessati devono essere sempre informati del trattamento effettuato dal Titolare.
2) A tal fine il Titolare utilizzerà una informativa cosiddetta di "primo" e di "secondo livello".
3) 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. Detto cartello riporterà le informazioni più importanti, comprese quelle di maggior impatto per l'interessato (es. finalità 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.
4) In presenza di più dispositivi di acquisizione, in relazione alla vastità dell'area e alle modalità delle riprese, potranno essere installati più cartelli informativi.
5) 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.
6) Quanto all'informativa di "secondo livello", essa verrà resa disponibile in luogo facilmente accessibile all'interessato, come ad esempio il sito istituzionale dell'Ente, e dovrà contenere tutte le informazioni obbligatorie previste dall'art. 13 RGPD e all'art. 10 del D. Lgs. n. 51/18.

7) 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.

22. 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 agli artt. 13 RGPD e 10 D. Lgs. 51/18;

c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 del RGPD o all'art. 12 del D. Lgs. n. 51/18, in particolare la cancellazione 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 oppure la trasformazione in forma anonima;

d) di opporsi, nei casi previsti dal RGPD, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21 del RGPD. Il Titolare del Trattamento 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 o all'art. 14 del D. Lgs. 51/18. 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 Titolare del trattamento 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 Titolare del Trattamento, ovvero l'incaricato specificamente designato, 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 e 14, 2° co, lett. d) del D. Lgs. 51/18.

5) Qualora il Titolare del Trattamento, ovvero l'incaricato specificamente designato, non sia in grado di identificare l'interessato o in caso di richieste eccessive o manifestamente infondate da parte dell'interessato, 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) Resta ferma la disciplina prevista dalla normativa nazionale ed europea in materia di limitazioni dell'esercizio di diritti dell'interessato.

10) 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.

CAPO VI – OBBLIGHI DEL TITOLARE

23. 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.

24. 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 VII – ALTRE DISPOSIZIONI

25. 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 resa nota agli interessati.

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

a) adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del Titolare, comunque non inferiore a sei mesi;

b) separazione logica dei dati registrati dai diversi titolari.

3) 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.

26. Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

1) Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, 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.

27. 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.

28. Entrata in vigore e norme di rinvio

1) Il presente Regolamento entrerà in vigore trascorsi 60 giorni dalla esecutività 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 citato nel presente Regolamento si rinvia alle fonti primarie costituite dal D. Lgs. 196/2003 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, dal RGPD e dal 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 del Ministero dell'interno.