Comune di Settimo Milanese

Regolamento per la disciplina e l'utilizzo degli impianti di videosorveglianza

Approvato con deliberazione del Consiglio Comunale n. 16 del 08/06/2020

Premessa

Il presente Regolamento nasce per disciplinare l'installazione e l'utilizzo dei sistemi di videosorveglianza da parte dell'Ente locale e per rispondere alla sempre crescente domanda di sicurezza da parte di cittadini.
Negli ultimi anni si sta assistendo a un'implementazione degli incentivi economici statali e regionali che sostengono progetti indirizzati a incrementare forme di difesa passiva mediante l'impiego di dispositivi deterrenti atti a prevenire e individuare fenomeni criminosi e vandalici. In tale direzione si registrano numerosi interventi legislativi che hanno attribuito a Sindaci e Comuni specifiche competenze in materia di tutela dell'incolumità pubblica e di sicurezza urbana. L'accento su tali sistemi è spesso posto nei Protocolli e nei Patti per la sicurezza urbana i quali confermano il peculiare interesse collettivo per le loro finalità e l'utilizzo.
L'esigenza di sicurezza manifestata dalla collettività cittadina, che richiede risposte concrete ed efficaci, è certamente da annoverare tra le priorità della convivenza civile e, come tale, induce riflessioni approfondite e condivise per l'indubbia rilevanza che la caratterizza. A tal proposito questo Regolamento si propone come frutto di una riflessione che è stata finalizzata ad un'analisi qualitativa dei processi decisionali orientati all'utilizzo dei sistemi di videosorveglianza, allo scopo di poter meglio indirizzare le autorità competenti attraverso l'individuazione delle migliori prassi da eseguire. Si è pertanto elaborato un documento unico di lavoro, sulla scorta delle disposizioni legislative vigenti, avendo riguardo particolare alla tutela della privacy di ogni singola persona così come chiaramente imposta dalla normativa vigente, privacy intesa come un complesso percorso di maturazione giuridica che possa coniugare il diritto alla riservatezza personale col dovere della pubblica amministrazione di proteggere i propri cittadini nei modi meno invasivi possibili. In questo contesto si inserisce la presente disciplina dell'utilizzo dei sistemi di videosorveglianza come strumento di tutela del territorio del Comune di Settimo come valido supporto al Corpo di Polizia Locale e alle forze di Polizia nell'attività investigativa delegata dall'Autorità Giudiziaria e/o d'iniziativa.
Molteplici sono i campi di applicazione individuati dal presente Regolamento: dal sistema di controllo e lettura delle targhe dei veicoli in entrata e uscita dal territorio comunale ai dispositivi (denominati "foto trappole") per l'individuazione dei soggetti che abbandonano rifiuti sul suolo pubblico, dalle "body cam" in uso agli appartenenti al Corpo di Polizia Locale alle telecamere da cruscotto (comunemente "dash cam") installate sulle auto di servizio.
In considerazione della particolare delicatezza della materia, anche per i riflessi ricadenti sulla sfera della riservatezza dei cittadini, tale Regolamento vuole essere un dispositivo coerente con il trattamento dei dati personali, nel rispetto dei diritti, delle libertà fondamentali e della dignità dei cittadini, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione degli stessi. In esso sono parimenti garantiti i diritti delle persone giuridiche e di ogni altro Ente o Associazione coinvolti nel trattamento, con riferimento alle norme di legge che sono di seguito illustrate.

Indice

Titolo Quarto

Tutele

Titolo Primo
Disposizioni generali

Art. 1 Oggetto

Il presente Regolamento disciplina il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza installati e attivati nel territorio comunale di competenza del Comune di Settimo Milanese, il quale garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Corpo di Polizia Locale, si svolga nel rispetto dei diritti, delle libertà fondamentali e, con particolare riferimento alla riservatezza e all'identità personale, nel rispetto della dignità delle persone fisiche e giuridiche coinvolte nel trattamento. Per tutto quanto non è dettagliatamente disciplinato nel presente Regolamento, si rinvia al disposto di cui al D.Lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" e successive modificazioni e integrazioni.

Art. 2 Finalità

La finalità della videosorveglianza è la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini che configura un trattamento di dati personali. E' considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione. La videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

- Protezione degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati e della microcriminalità commessa nel territorio comunale nell'ambito della "sicurezza urbana" di cui all'articolo 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;
- Razionalizzazione e miglioramento dei servizi al pubblico volti ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;
- Protezione della proprietà del demanio pubblico e privato;
- Rilevazione, prevenzione e controllo delle infrazioni a leggi e regolamenti;
- Rilevazione, prevenzione e controllo di fenomeni di degrado e abbandono di rifiuti, in modo da poter svolgere controlli volti ad accertare e sanzionare le violazioni delle norme contenute prevalentemente nel regolamento di polizia urbana, nei regolamenti locali in genere e nelle ordinanze sindacali;
- Verifica, controllo e gestione dell'accesso a zone a traffico limitato, ove sussistenti;
- Acquisizione di prove penalmente e/o amministrativamente rilevanti anche a supporto delle forze di Polizia;
- Vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
- Tutela dell'ordine, del decoro e della quiete pubblica;
- Controllare aree specifiche del territorio comunale;
- Monitorare, rilevare e analizzare i flussi di traffico veicolare;

- Attivazione di misure volte alla limitazione alla circolazione dei veicoli al fine di ridurre l'inquinamento atmosferico;
- Verificare e calibrare il sistema di gestione centralizzata degli impianti semaforici;
- Controllo di aree urbane ritenute di particolare interesse o in cui si rilevano situazioni di pericolo, degrado, spaccio di stupefacenti, prostituzione, occupazione abusiva d'immobili o che, in qualunque modo, favoriscono o possono favorire l'insorgere di situazioni criminose.

Art. 3 Definizioni

- Dati personali: qualsiasi informazioni concernenti una persona fisica identificata o identificabile anche indirettamente, oppure riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari;
- Dati identificativi: dati che consentono l'identificazione diretta dell'interessato (esempio: nome e cognome, indirizzo e-mail, indirizzo di casa, numero del documento personale o del veicolo, data di nascita, identità digitale, numero di telefono);
- Dati soggetti a trattamento speciale: dati che prevedono un consenso esplicito, anche se non necessariamente scritto, che riguardano aspetti particolarmente privati dell'individuo la cui tutela ha lo scopo di garantire la libertà di pensiero e di opinione, la sua dignità e la libertà da possibili discriminazioni (esempio: dati genetici, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati giudiziari, dati relativi alla salute);
- Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- Dati anonimi: dati privati di tutti gli elementi identificativi che, pertanto, non sono soggetti alle norme di tutela;
- Dati pseudonimi: dati personali nei quali gli elementi identificativi sono stati sostituiti da elementi diversi quali stringhe di caratteri o numeri (*hash*), oppure sostituendo al nome uno pseudonimo (*nickname*), purché sia tale da rendere estremamente difficoltosa l'identificazione dell'interessato;
- Minimizzazione: raccolta dei soli dati pertinenti, limitando quindi il trattamento a ciò che è realmente necessario e indispensabile rispetto alla finalità alla quale sono destinati;
- Interessato: persona a cui si riferisce il trattamento dei dati che può essere solo una persona fisica, non giuridica;
- Autorità di controllo: Garante della privacy di cui all'articolo 14 del presente Regolamento;
- Destinatario: soggetto che riceve dati personali dal titolare, siano essi interni o esterni; il destinatario può ricevere tali dati per eseguire trattamenti per conto del titolare o per conseguire proprie specifiche finalità;
- Profilazione: elaborazione dei dati relativi a uno o più soggetti allo scopo di suddividerli in gruppi omogenei in base a gusti, interessi e comportamenti;
- Pseudonimizzazione: trattamento dei dati personali in modo tale che non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che le

stesse siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- Titolare del trattamento: persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità e modalità del trattamento di dati personali, nonché agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- Responsabile del trattamento: persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento; nel nuovo Regolamento Europeo 2016/679 è definito *data processor* e si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
- Incaricato del trattamento: persona fisica autorizzata a compiere le operazioni di trattamento dal titolare o dal responsabile;
- Interessato: persona fisica a cui si riferiscono i dati personali il quale, per l'esercizio dei propri diritti, può rivolgersi direttamente al titolare del trattamento anche in un momento successivo a quello in cui ha prestato il consenso, potendo così revocarlo anche se già prestato;
- Comunicazione: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- Diffusione: dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 4 Tipologie di trattamento

- Raccolta dei dati: è la prima operazione e generalmente rappresenta l'inizio del trattamento; consiste nell'attività di acquisizione del dato;
- Registrazione: memorizzazione dei dati su un qualsiasi supporto;
- Organizzazione: classificazione dei dati secondo un metodo prescelto;
- Strutturazione: attività di distribuzione dei dati secondi schemi precisi;
- Conservazione: memorizzare le informazioni su un qualsiasi supporto;
- Consultazione: lettura dei dati personali compresa la semplice visualizzazione dei dati;
- Elaborazione: attività con la quale il dato personale subisce una modifica sostanziale;
- Modificazione: elaborazione che può riguardare anche solo parte minima del dato personale;
- Selezione: individuazione di dati personali nell'ambito di gruppi di dati già memorizzati;
- Estrazione: attività di estrapolazione di dati da gruppi già memorizzati;
- Raffronto: operazione di confronto tra dati, sia in conseguenza di elaborazione che di selezione o consultazione;
- Utilizzo: attività generica che ricopre qualsiasi tipo d'impiego di dati;
- Interconnessione: utilizzo di più banche dati con impiego di strumenti elettronici;
- Blocco: conservazione con sospensione temporanea di ogni altra operazione di trattamento;

- Comunicazione o cessione: dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati. In caso di comunicazione il dato é trasferito a terzi;
- Diffusione: dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione; si ha, quindi, diffusione anche quando si pubblica online, ad esempio una fotografia su un social network, ed in assenza di consenso tale attività deve ritenersi illecita;
- Cancellazione: eliminazione di dati tramite utilizzo di strumenti elettronici;
- Distruzione: attività di eliminazione definitiva dei dati.

Art. 5 Ambito di applicazione

Il presente Regolamento disciplina il trattamento dei dati ottenuti mediante gli impianti di videosorveglianza presenti e attivati nel territorio urbano ed extraurbano di competenza del Comune di Settimo Milanese, collegato alla sala di controllo del Comando di Polizia Locale.

Art. 6 Normative di riferimento

- D.Lgs. 10 agosto 2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- D.Lgs. 18 maggio 2018, n. 51, "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";
- DPR 15 gennaio 2018, n. 15, "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";
- Legge 18 aprile 2017, n. 48, "Disposizioni urgenti in materia di degrado delle città";
- Direttiva UE 2016/680 del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai 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;
- Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 26 aprile 2016 (GDPR General Data Protection Regulation), in vigore dal 25 maggio 2018, 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 (regolamento generale sulla protezione dei dati);

- Circolare 2 marzo 2012, n. 558/SICPART/421.2/70/224632, Direttiva del Ministero dell'Interno sui sistemi di videosorveglianza in ambito comunale;
- Provvedimento in materia di videosorveglianza del Garante per la protezione dei dati personali dell'8 aprile 2010;
- Legge 23 aprile 2009, n. 38, "Conversione in legge, con modificazioni, del decreto-legge 23 febbraio 2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori";
- D.Lgs. 3 aprile 2006, n. 152, "Norme in materia ambientale";
- D.Lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali";
- D.Lgs. 18 agosto 2000, n. 267, "Testo unico delle leggi sull'ordinamento degli enti locali";
- D.Lgs. 30 aprile 1992, n. 285, "Nuovo codice della strada" e successive modifiche e integrazioni, ed in particolare all'art. 200, in riferimento al controllo lettura targhe, è stabilito che, le infrazioni alle presente legge, quando è possibile, devono essere immediatamente contestate tanto al trasgressore quanto alla persona che sia obbligata in solido al pagamento della somma dovuta;
- Legge 7 agosto 1990, n. 241, "Nuove norme sul procedimento amministrativo";
- Legge 7 marzo 1986, n. 65, "Legge quadro sull'ordinamento della Polizia Municipale";
- Legge 24 novembre 1981, n. 689, "Modifiche al sistema penale";
- Legge 20 maggio 1970, n. 300, "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento", la quale dispone che 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.

Art. 7 Modalità di raccolta e conservazione dei dati personali

I dati personali oggetto di trattamento sono trattati per le finalità di cui all'articolo 2 del presente Regolamento e secondo i seguenti principi:

- Liceità: ogni trattamento deve trovare fondamento in un'idonea base giuridica;
- Correttezza e trasparenza: il responsabile del trattamento dei dati fornisce agli interessati alcune informazioni per metterli in condizioni di esercitare i propri diritti;
- Limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- Minimizzazione dei dati: i dati devono essere adeguati, pertinenti, limitati e funzionali a quanto necessario rispetto alle finalità del trattamento;
- Esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- Limitazione della conservazione: provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- Integrità e riservatezza: garanzia di sicurezza adeguata dei dati personali oggetto del trattamento.

Ai titolari è affidato il compito di decidere autonomamente circa le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce dei criteri specifici indicati nel presente Regolamento. Fra questi la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
Le immagini video delle unità di ripresa sono inviate presso la sede del Corpo di Polizia Locale di Settimo Milanese dove sono registrate su appositi server.
I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono sovrascritti con modalità automatica e, quindi, cancellati. La conservazione dei dati personali per un tempo superiore è ammessa esclusivamente su specifica richiesta dell'Autorità Giudiziaria o di Polizia Giudiziaria in relazione ad un'attività investigativa in corso.
Alle immagini raccolte possono accedere, per l'espletamento delle relative indagini, gli appartenenti all'Amministrazione Giudiziaria, le persone da essi espressamente autorizzate e gli organi di Polizia. Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino copia delle riprese effettuate, devono presentare un'istanza scritta e motivata indirizzata al Responsabile della gestione e del trattamento dei dati.

Art. 8 Valutazione d'impatto sul trattamento dei dati

La valutazione d'impatto sulla protezione dei dati è eseguita dal titolare del trattamento con il responsabile della protezione dati, qualora ne sia designato uno, ai sensi del Regolamento Europeo 2016/679.
La valutazione del rischio, da realizzare per ogni singolo trattamento, dovrà portare il titolare a decidere in autonomia se sussistono rischi elevati inerenti il trattamento, in assenza dei quali potrà procedere oltre. Se invece ritenesse sussistenti rischi per le libertà e i diritti degli interessati, dovrà individuare le misure specifiche richieste per attenuare o eliminare tali rischi.
Solo nel caso in cui il titolare non dovesse trovare misure idonee a eliminare o ridurre il rischio, occorrerà consultare l'Autorità di controllo che interverrà successivamente al trattamento sulle valutazioni del titolare, indicando le misure ulteriori eventualmente da implementare, fino ad ammonire, se del caso, il titolare o vietare il trattamento.
La valutazione d'impatto va sviluppata solo per particolari trattamenti, cioè quando il trattamento prevede l'uso di nuove tecnologie che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto previsto sul trattamento e la protezione dei dati personali considerati la natura, l'oggetto, il contesto e le finalità del trattamento, e che ciò può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
E' eseguita una valutazione sistematica e globale di:

- aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- categorie particolari di dati personali sensibili o giudiziari, di zone a larga scala accessibili al pubblico, di fatti costitutivi illeciti amministrativi e/o penali.

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati e comunica tali elenchi al comitato europeo per la comunicazione dei dati. Inoltre può redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati.

La valutazione contiene almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati.

Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

I dati trattati devono essere notificati al Garante solo se rientrano nei casi specificatamente previsti dalla normativa vigente sulla privacy. A tale proposito la normativa prevede che non vadano comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardino immagini conservate temporaneamente per esclusive finalità di sicurezza pubblica o di tutela delle persone e del patrimonio.

Titolo Secondo
Soggetti

Art. 9 Soggetti coinvolti

I soggetti coinvolti nel trattamento dei dati personali sono i seguenti:

- Titolare del trattamento dei dati;
- Responsabile del trattamento dei dati;
- Responsabile della protezione dati;
- Persone autorizzate al trattamento dei dati;
- Autorità;
- Soggetti esterni;
- Interessati.

Art. 10 Titolare del trattamento dei dati

Titolare del trattamento dei dati è il Comune di Settimo Milanese, rappresentato dal Sindaco, il quale determina:

- le finalità e i mezzi del trattamento di dati personali;
- definisce le linee organizzative per l'applicazione della normativa di settore;
- effettua le notificazioni al Garante per la protezione dei dati personali;
- nomina i responsabili dei dati trattati acquisiti mediante l'utilizzo degli impianti di videosorveglianza, impartendo istruzioni ed assegnando compiti e responsabilità;
- detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;
- vigila sulla puntuale osservanza delle disposizioni impartite.

Art. 11 Responsabile del trattamento dei dati

Il Comandante del Corpo di Polizia Locale di Settimo Milanese, o altri soggetti individuati dal Sindaco, è designato quale responsabile del trattamento dei dati personali trattati, per conto del titolare di cui all'articolo precedente, mediante l'utilizzo degli impianti di videosorveglianza descritti nel titolo terzo e secondo le disposizioni di cui all'articolo 7 del presente Regolamento.
La nomina è effettuata con atto del Sindaco, nel quale sono analiticamente specificati i compiti affidati ai responsabili.
I compiti del responsabile del trattamento dei dati sono:

- individuare e nominare con propri atti i soggetti autorizzati al trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto trattamento dei dati;

- istruire e formare tali soggetti 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;
- controllare che il trattamento dei dati, effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui agli articoli 7 e 8 del presente Regolamento;
- assistere il titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato garantendo 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;
- se 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 anche per assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico;
- assicurare 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;
- assistere 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 e nella valutazione di impatto sulla protezione dei dati ai sensi dell'articolo 8 del presente Regolamento;
- garantire 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 impegnandosi ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;
- mettere 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;
- 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;
- garantire la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale autorizzato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del responsabile della protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali.

Art. 12 Responsabile della protezione dei dati

Il Comandante del Corpo della Polizia Locale di Settimo Milanese, o altri soggetti individuati dal Sindaco, è designato anche quale responsabile della protezione dei dati.
Il Comandante può anche nominare un responsabile della protezione dati personali, con atto scritto, in funzione della qualità professionali, in particolare della conoscenza specialistica della normativa e delle

prassi in materia di protezione dei dati e delle capacità di assolvere i compiti e le finalità di cui all'articolo 2 del presente Regolamento.
Egli ha il compito di facilitare le persone autorizzate al trattamento dei dati, di cui all'articolo 13 del presente Regolamento, nel trattamento dei dati personali in osservanza alla corretta applicazione della normativa vigente in materia.

Art. 13 Persone autorizzate al trattamento dei dati

Le persone autorizzate al trattamento dei dati sono individuate dal Sindaco e/o dal Comandante del Corpo di Polizia Locale di Settimo Milanese, congiuntamente al responsabile della protezione dei dati, in numero sufficiente a garantire il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento.
I soggetti autorizzati sono designati tra gli appartenenti al Corpo di Polizia Locale che rivestono la qualifica di Agenti o Ufficiali di Polizia Giudiziaria i quali devono garantire, nello svolgimento dei compiti assegnati, il pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati. Questi, per l'accesso alle banche dati informatiche, possono essere dotati di proprie credenziali personali che devono essere mantenute riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria *password* inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento. Devono altresì conservare i supporti informatici contenenti dati personali in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi e mantenere la massima riservatezza sui dati personali dei quali vengano a conoscenza nello svolgimento delle funzioni istituzionali.
In assenza di proprie credenziali personali di accesso al sistema di videosorveglianza, il titolare del trattamento è tenuto a vigilare sul corretto utilizzo dei sistemi di videosorveglianza nel rispetto della normativa vigente in riferimento all'articolo 6 del presente Regolamento.
Ogni operatore deve custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.
E' necessario evitare la creazione di banche dati senza autorizzazione espressa del responsabile dei dati trattati o fuori dai casi previsti dagli articoli 2, 6 e 7 del presente Regolamento.
Ogni soggetto autorizzato al trattamento dei dati deve, a richiesta, fornire al responsabile dei dati trattati ed al responsabile della protezione dei dati, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Art. 14 Autorità

Il Garante per la protezione dei dati personali, in altre parole il Garante Privacy, è l'autorità di controllo nazionale italiana. E' autorità amministrativa indipendente istituita dalla Legge 31 dicembre 1996, n. 675, in attuazione della direttiva comunitaria 95/46/CE, e disciplinata dal D.Lgs. 30 giugno

2003, n.196, “Codice in materia di protezione dei dati personali”. La sua sede è a Roma, Piazza di Monte Citorio n. 121.
Secondo quanto disposto dall’art. 154 del D.Lgs. 196/2003, si occupa di:

- verificare la conformità alla legge dei trattamenti e prescrivere ai titolari le misure da adottare;
- esaminare i reclami;
- limitare, sospendere o vietare i trattamenti in violazione delle norme;
- adottare le autorizzazioni generali;
- promuovere codici di deontologia e buona condotta;
- partecipare alle attività comunitarie e internazionali;
- irrogare sanzioni correttive.

Art. 15 Soggetti esterni

Qualora un responsabile del trattamento ricorra a un altro responsabile del trattamento, come eventualmente possibile nell’ipotesi indicata all’articolo 17 del presente Regolamento, per l’esecuzione di specifiche attività di trattamento per conto del titolare, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell’Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l’altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l’intera responsabilità dell’adempimento degli obblighi dell’altro responsabile.
Mediante apposita disposizione scritta, il titolare del trattamento dei dati è obbligato a nominare ogni soggetto esterno come:

- responsabile esterno del trattamento;
- amministratore di sistema, quando ne ricopra il ruolo;
- autonomo titolare del trattamento, quando ne sussistano i requisiti o come subordine nel caso di mancata accettazione della nomina a responsabile.

Art. 16 Amministratori di sistema

Qualora dovessero presentarsi problemi informatici, al titolare del trattamento e/o all’eventuale responsabile nominato spetta il compito di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio di cui all’art. 32 del GDPR (qui riportato: “*Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (...)*”) avvalendosi se del caso di un amministratore di sistema. Egli é una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui

vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi *software* complessi e di organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. Questi deve essere nominato con atto formale e rispondere del proprio operato ai requisiti imposti dalla normativa ed essere monitorato costantemente dal titolare del trattamento.

Art. 17 Interessati

Sono interessati tutti i soggetti a cui si riferiscono i dati personali.
I diritti in capo ad essi sono meglio evidenziati negli articoli 28 e 28-bis del presente Regolamento.

Art. 18 Accordi di contitolarità

Al fine di promuovere la sicurezza integrata sul territorio, ovvero di concorrere alla promozione e all'attuazione di un sistema unitario e integrato di sicurezza per il benessere e la valorizzazione delle comunità territoriale del Comune di Settimo Milanese, possono essere individuati specifici obiettivi per incrementare il controllo del territorio anche attraverso il concorso, sotto il profilo di sostegno strumentale, finanziario e logistico, di soggetti pubblici e privati per lo svolgimento di attività di interesse comune con la collaborazione tra le forze di Polizia e la Polizia Locale.
Ai sensi dell'art. 26 del GDPR, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato il quale può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Titolo Terzo
Tipologie di sistemi

Art. 19 Sistemi di videosorveglianza

I sistemi di videosorveglianza individuati dal presente Regolamento sono:

- di lettura targhe dei veicoli;
- da cruscotto a bordo veicolo, definiti “dash cam”;
- per operatori di Polizia Locale a bordo uomo, definiti “body cam”;
- di contrasto all’abbandono dei rifiuti, definiti “foto trappole”;
- di controllo interno e/o esterno delle strutture demaniali;
- altre tipologie che possono essere individuate in base ai criteri stabiliti dall’art. 24.

Art. 20 Lettura targhe dei veicoli

Tale dispositivo di videosorveglianza è uno strumento gestito direttamente dagli operatori del Corpo di Polizia Locale come supporto nella protezione degli utenti della strada e nell’accertamento delle violazioni relative alla circolazione dei veicoli.

Il *software* del sistema di cui al presente articolo può essere installato su una telecamera semplice o su un dispositivo specifico. La telecamera può essere posizionata su un supporto fisso e può essere utilizzata in movimento; questa scansiona le targhe e le invia al server collegato al Ministero dei Trasporti, all’IVASS e al Ministero dell’Interno. Le informazioni sulle targhe trasmesse vengono poi inviate immediatamente su dispositivo *tablet* o *mobile phone* in dotazione agli operatori in servizio, per la verifica in tempo reale.

Ai sensi dell’art. 200 del D.Lgs. 285/1992 e nel rispetto delle circolari ministeriali diramate in materia, il dispositivo in oggetto ha la funzione di accertamento diretto delle violazioni, così da procedere alla contestazione immediata da parte degli operatori che ne stanno facendo uso, nel momento immediatamente successivo al transito del veicolo. Nella situazione di fatto che renda impossibile la contestazione immediata, devono essere dettagliatamente indicate nel verbale di accertamento le motivazioni che non l’hanno consentita.

Riguardo la conservazione dei fotogrammi si richiamano i contenuti del provvedimento del Garante della protezione dei dati personali dell’8 aprile 2010, nonché l’articolo 7 del presente Regolamento.

Art. 21 Dash cam

La dash cam, contrazione di dashboard camera (telecamera da cruscotto), è un dispositivo elettronico per l’acquisizione di immagini, applicabile sul parabrezza o sullo specchietto retrovisore dei veicoli di servizio in uso alla Polizia Locale di Settimo Milanese che sono utilizzate al fine di registrare gli eventi che accadono all’esterno della vettura nella direzione in cui tale dispositivo è rivolto.

Esse sono tutte dotate di apposita fessura per l'inserimento di un dispositivo elettronico di registrazione, ovvero "micro SD", essenziale per registrare i filmati. Questo sistema di videosorveglianza si alimenta tramite porta USB o presa accendisigari dell'auto. Le immagini video che sono ritenute utili ai fini di polizia giudiziaria o amministrativa devono essere salvate su supporto informatico non trascrivibile e conservate secondo le finalità di cui all'articolo 2 e nel rispetto delle indicazioni di cui all'articolo 7 del presente Regolamento, le altre sono sovrascritte automaticamente e, quindi, cancellate.
Le dash cam sono utilizzate nel rispetto di quanto prescritto con nota del Garante della protezione dei dati personali protocollo n. 49612 del 26 luglio 2016 il cui trattamento dei dati è ricondotto nell'ambito dell'art. 53 del D.Lgs 196/2003 trattandosi di dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica e di polizia giudiziaria.

Art. 22 Body cam

Le body cam sono delle telecamere portatili, che si posizionano sulle divise degli operatori di Polizia Locale, al fine di monitorare l'attività di chi le indossa e dei soggetti con cui interagiscono. Tali micro camere sono attivabili dagli operatori durante lo svolgimento del servizio assegnato mediante pressione di un tasto posto sull'apparecchio stesso e disattivabili nella medesima modalità, ogni volta che l'operatore lo ritenga opportuno al fine di salvaguardare il proprio operato e monitorare situazioni di criticità, turbativa e illegalità, dandone preventiva comunicazione orale agli interessati. Le immagini video che sono ritenute utili ai fini di polizia giudiziaria o amministrativa devono essere salvate su supporto informatico non trascrivibile e conservate secondo le finalità di cui all'articolo 2 e nel rispetto delle indicazioni di cui all'articolo 7 del presente Regolamento, le altre sono sovrascritte automaticamente e, quindi, cancellate.
Le body cam sono utilizzate nel rispetto di quanto prescritto con nota del Garante della protezione dei dati personali protocollo n. 49612 del 26 luglio 2016 il cui trattamento dei dati è ricondotto nell'ambito dell'art. 53 del D.Lgs 196/2003 trattandosi di dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica e di polizia giudiziaria.
In merito alle precise modalità di utilizzo si rimanda alla disposizione di servizio interna protocollo n. 17/04 del 03 giugno 2019.

Art. 23 Foto trappole

Le foto trappole (o telecamere modulari) sono sistemi di videosorveglianza che si basano sulla rilevazione di movimento all'interno di una determinata area di ripresa, sia di giorno che di notte, grazie a led infrarossi invisibili ad occhio umano. Le immagini video sono registrate e successivamente estrapolate dal dispositivo stesso o, eventualmente, trasmesse a distanza, grazie ad una rete gsm o wi-fi. Il dispositivo si attiva grazie ad un sensore al passaggio di un corpo.
Esse sono utilizzate con lo scopo di contrastare l'abbandono di rifiuti o il loro errato/non autorizzato conferimento e devono essere posizionate nel territorio comunale con l'obiettivo di prevenire e/o reprimere tali azioni al fine di avviare le successive verifiche utili ad accertare eventuali violazioni amministrative e/o penali.

L'attivazione del dispositivo, che è finalizzata ad attività di polizia giudiziaria e amministrativa, comporta gli obblighi d'informativa con cartelli posti prima del raggio d'azione della telecamera, secondo le prescrizioni del Regolamento Europeo 2016/679 nonché dell'articolo 25 del presente Regolamento.
L'uso di foto trappole per la prevenzione e il contrasto del fenomeno dell'abbandono incontrollato dei rifiuti, senza l'utilizzo di cartelli informativi, di cui al citato articolo 25 del presente Regolamento, nell'espletamento di funzioni di polizia giudiziaria, è consentito nelle seguenti ipotesi:

- illecita gestione di rifiuti e loro depositi incontrollati, punibili ai sensi dell'art. 256 del D.Lgs. 152/2006;
- illecita combustione di rifiuti, punibile ai sensi dell'art. 256-bis del D.Lgs. 152/2006.

Il loro utilizzo è lecito solo se non risulta possibile, o si riveli inefficace e inattuabile, il ricorso a sistemi di controllo e monitoraggio del rispetto delle disposizioni considerando le modalità, tipologie ed orario di deposito dei rifiuti.
Le immagini video che sono ritenute utili ai fini di polizia giudiziaria o amministrativa devono essere salvate su supporto informatico non trascrivibile e conservate secondo le finalità di cui all'articolo 2 e nel rispetto delle indicazioni di cui all'articolo 7 del presente Regolamento, le altre sono sovrascritte automaticamente e, quindi, cancellate.

Art. 24 Controllo interno e/o esterno delle strutture pubbliche

Fatto salvo quanto previsto dal presente Regolamento, il Comune di Settimo Milanese, a tutela delle aree interne ed esterne delle proprie infrastrutture (uffici, stabili comunali e loro pertinenze), può prevedere e installare delle telecamere di videosorveglianza in zone sensibili opportunamente individuate, dove possono accedere solo persone autorizzate, un sistema di controllo per prevenire potenziali attacchi interni ed esterni alle infrastrutture pubbliche, nonché per la salvaguardia dell'incolumità degli operatori del Corpo di Polizia Locale e, più in generale, dei dipendenti e degli amministratori comunali, sempre nel rispetto della Legge 300/1970, la quale dispone che gli impianti di videosorveglianza non possono essere utilizzati per effettuare controlli sull'attività lavorativa.

Art. 25 Altre tipologie

Possono altresì essere individuate, dal titolare del trattamento dei dati di concerto con le figure di cui agli articoli 11, 12 e 13, in relazione alla specificità dei contesti e secondo le finalità di cui all'articolo 2 del presente Regolamento, altre tipologie di videosorveglianza tenuto conto anche delle esigenze delle aree rurali confinanti con il territorio urbano.

Titolo Quarto
Tutele

Art. 26 Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata. A tal fine è possibile utilizzare lo stesso modello d'informativa indicante il titolare del trattamento e la finalità perseguita, ai sensi dell'art. 13 del D.Lgs 196/2003, il cui fac-simile è reperibile tra gli allegati del provvedimento in materia di videosorveglianza del Garante per la protezione dei dati personali dell'8 aprile 2010, di seguito riprodotti.

Il modello è adattabile a varie circostanze.

In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli posizionati all'ingresso del territorio comunale di competenza di Settimo Milanese o dove il titolare del trattamento dei dati personali lo ritenga opportuno secondo le modalità e le finalità rappresentate nel presente Regolamento e qui riportate:

- il cartello deve essere collocato all'inizio del territorio comunale di competenza prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

L'informativa, resa in forma semplificata avvalendosi del predetto modello, rinvia al testo completo di cui al presente Regolamento, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici, in particolare, tramite il sito istituzionale del Comune di Settimo Milanese.

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.

Le telecamere installate nei singoli punti o zone di rilevamento targhe sono di tipologia fissa e indicate sul sito istituzionale del Comune di Settimo Milanese. Il tempo di conservazione delle immagini è per un periodo

massimo di 7 giorni successivi alla rilevazione delle informazioni e delle immagini raccolte, così come indicato all'articolo 7 del presente Regolamento, e conservate per un periodo di tempo non superiore a quello necessario per il conseguimento delle finalità di polizia, dopodiché vengono automaticamente cancellate dal sistema informatico. I dati personali soggetti a trattamento automatizzato, trascorso il tempo sopra indicato, sono accessibili ai soli operatori a ciò abilitati e designati, incaricati del trattamento secondo profili di autorizzazione predefiniti, come indicato nel titolo secondo del presente Regolamento, in relazione a specifiche attività informative, di sicurezza o di indagine di polizia giudiziaria. Le apparecchiature informatiche che si occupano della gestione ed archiviazione dei dati acquisiti dal sistema di videosorveglianza sono installate entro un locale ad accesso controllato presente nel comando di Polizia Locale di Settimo Milanese. Tale sistema, senza necessità di modificare il presente Regolamento, potrà essere ulteriormente implementato, secondo le necessità e le esigenze future, nel rispetto del provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010 e della direttiva del Ministero dell'Interno del 2 marzo 2012. Gli apparati acquistati e installati dal Comune sono e saranno gestiti direttamente dalla Polizia Locale.

Art. 27 Accesso agli impianti di controllo e ai dati

L'accesso agli impianti di videosorveglianza di cui al presente Regolamento è consentito solo agli operatori di Polizia Locale del Comune di Settimo Milanese e alle persone autorizzate dal responsabile e dal titolare del trattamento dei dati mediante l'utilizzo di apposite credenziali.
L'accesso ai dati è consentito solo ai seguenti soggetti:

- al titolare del trattamento;
- al responsabile e agli incaricati dello specifico trattamento;
- all'Autorità Giudiziaria o alla Polizia Giudiziaria per finalità d'indagine debitamente autorizzata dal titolare o dal responsabile del trattamento;
- all'amministratore del sistema, individuato dalla ditta incaricata della manutenzione degli impianti;
- al terzo, se autorizzato, in quanto oggetto delle riprese.

Questi dovrà avere visione solo delle immagini che lo riguardano direttamente. Al fine di evitare l'accesso a immagini riguardanti altri soggetti dovrà essere utilizzata, da parte dell'incaricato al trattamento, una schermatura del video, tramite opportune accortezze.

Art. 28 Diritti degli interessati

Ai sensi della Legge 241/1990, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente, gli interessati, dietro presentazione di apposita istanza da presentarsi presso il protocollo del Comune di Settimo Milanese, hanno diritto di:

- ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;
- prendere visione ed estrarre copia dei documenti amministrativi in cui abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso, mediante la presentazione di una richiesta motivata;

- essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
- ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati;
- ottenere la cancellazione, 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;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Per ciascuna di esse può essere chiesto all'interessato un contributo spese secondo le modalità previste dalla normativa vigente e visionabili sul sito istituzionale del Comune di Settimo Milanese nella sezione dedicata all'accesso agli atti.

Nell'esercizio dei diritti sopra descritti l'interessato può conferire per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. Le istanze di cui al presente articolo possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata o posta elettronica certificata.

Il termine per la risposta all'interessato è, per tutti i diritti, compreso il diritto di accesso, pari a 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Art. 28-bis Procedura per l'accesso alle immagini da parte di terzi e diritti degli interessati

La persona interessata ad accedere alle immagini deve avanzare apposita istanza (il fac-simile è reperibile online sul sito del Comune) al responsabile del trattamento, indicato nell'informativa. Nell'istanza dovrà essere indicato a quale impianto di videosorveglianza si fa riferimento e la stessa dovrà essere presentata al protocollo del Comune di Settimo Milanese.

Il diritto di cui al comma precedente riferito alle immagini concernenti persone decedute può essere esercitato da chi ha un interesse proprio o agisce a tutela dell'interessato o per ragioni famigliari.

Nel caso le immagini di possibile interesse non siano oggetto di conservazione, di ciò dovrà essere data formale comunicazione al richiedente.

Nel caso le immagini di possibile interesse siano oggetto di conservazione, il richiedente dovrà fornire altresì ulteriori indicazioni, finalizzate a facilitare il reperimento delle immagini stesse, tra cui:

- il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa;
- il luogo ed i luoghi di possibile ripresa;
- la presenza di altre persone, una descrizione dell'attività svolta durante le riprese.

Nel caso che tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data comunicazione al richiedente.

Il responsabile del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente entro 15 giorni dalla richiesta. Nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui il suddetto potrà visionare le immagini che lo riguardano.

Nel caso il richiedente intenda sporgere reclamo per mancata ottemperanza degli uffici, dovrà presentare in forma libera, indirizzata al responsabile del trattamento, indicando i motivi del reclamo o rivolgersi al Garante della protezione dei dati personali.

Art. 29 Trattamento dei dati

Il Regolamento, come già previsto dal Codice in materia di protezione dei dati personali, prevede che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I dati personali dei soggetti interessati sono trattati nel rispetto delle modalità descritte all'articolo 7, con riferimento alle normative vigenti di cui all'articolo 6.

Art. 30 Limitazioni all'utilizzo dei dati

Il presente Regolamento stabilisce che i dati personali siano utilizzati secondo quanto necessario e rispettando le finalità di cui all'articolo 2, limitatamente alla loro conservazione in conformità al GDPR. Gli stessi possono essere potenzialmente limitati in qualunque momento da parte dell'Autorità Garante, ad eccezione della loro conservazione, e dall'interessato nei casi in cui ricorra una delle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali;
- i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, mentre al titolare del trattamento non servono più a fini del trattamento;
- l'interessato si è opposto al trattamento ed è in attesa delle verifiche necessarie per determinare se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato.

In ciascuno di questi casi i dati possono essere trattati soltanto ai fini della loro conservazione, a meno che:

- non vi sia il consenso dell'interessato;
- se tale trattamento sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria;
- per tutelare i diritti di un'altra persona fisica o giuridica;
- per motivi di interesse pubblico rilevante dell'Unione Europea o di uno Stato membro.

Nel caso in cui i dati personali oggetto di limitazione siano stati comunicati ad altri soggetti, è onere del titolare del trattamento darne comunicazione a ciascuno dei destinatari, tranne se ciò sia impossibile o implichi uno sforzo sproporzionato in riferimento all'art. 19 del GDPR. In ogni caso, il titolare del trattamento è tenuto a comunicare tali destinatari all'interessato che ne faccia richiesta.
In un secondo momento la limitazione può essere revocata; prima che la revoca sia efficace però, il titolare del trattamento deve avvisare l'interessato.

Art. 31 Tutela legale connessa al trattamento dei dati

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente Regolamento ha il diritto di proporre reclamo al titolare o al responsabile del

trattamento di questo Comune.
L'autorità di controllo cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale avverso la decisione presa che sia giuridicamente vincolante o nel caso in cui il reclamo non sia trattato o non sia stata comunicata risposta entro tre mesi.

Art. 32 Adempimenti in caso di violazione dei dati

Il titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare eventuali violazioni di sicurezza, documentandole, che comportino, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o trattati al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.
Il responsabile del trattamento che é a conoscenza di un'eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.
Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.
Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi e significativi sugli individui, causando danni fisici, materiali o immateriali fra i quali: la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

Art. 33 Disposizioni finali

Qualora dovessero intervenire modifiche normative o regolamentari in materia di videosorveglianza e trattamento dei dati personali, il presente Regolamento si aggiorna senza necessità di espressa modifica, escluso nel caso di variazione dell'assetto territoriale comunale.
Per quanto non previsto dal presente Regolamento, si fa rinvio alla Legge, ai suoi provvedimenti di attuazione, alle decisioni del Garante e ad altra normativa vigente, sia speciale che generale.
Il presente Regolamento entra in vigore alla data della sua approvazione da parte del Consiglio Comunale e abroga ogni disposizione precedente in materia.