COMUNE DI OLIENA

Provincia di Oliena

Regolamento per la disciplina ed utilizzo degli impianti di videosorveglianza

Approvato con D.C.C. n. del

INDICE

Art. 1 - Obiettivi e ambito di applicazione

1. Il presente regolamento disciplina le modalità di raccolta, trattamento, conservazione ed accesso dei dati personali mediante sistemi di videosorveglianza gestiti, nell'ambito del proprio territorio dal Comune di Oliena ed ha lo scopo di stabilire norme tecniche e organizzative di dettaglio e di concorrere a definire la base giuridica, le finalità e i mezzi del trattamento.
2. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, ossia a distanza, mediante dei dispositivi di ripresa video, collegati ad un centro di controllo.
3. Le immagini, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi la videosorveglianza incide sul diritto delle persone alla propria riservatezza.
4. Con il presente regolamento si garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti e impiegati dal comune nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; si garantiscono, altresì, i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento, avuto riguardo anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico
5. Le prescrizioni indicate nel presente documento vengono dettate in ottemperanza a quanto prescritto dalle seguenti fonti normative e Provvedimenti del Garante per la tutela dei dati personali:
   - Regolamento Ue 2016/679 (d'ora in poi GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
   - D.lgs. 196/2003 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali) ed allegato tecnico nella sua versione aggiornata al D.Lgs. 101/2018 e ss. mm.;
   - D.lgs. 51/2018 (d'ora in poi direttiva polizia) che ha recepito la direttiva Ue 2016/680 relativa alla protezione delle persone fisiche.
   - Provvedimento Generale sulla Videosorveglianza emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010 e ss. mm.
   - Linee Guida n. 3/2020 sul trattamento di dati personali attraverso la Videosorveglianza.
6. Il presente regolamento, ai sensi dell'articolo 5 del GDPR e articolo 3 della direttiva polizia, stabilisce norme di dettaglio rilevanti finalizzate ad attuare, a riguardo dei trattamenti dei dati personali effettuati mediante l'uso di sistemi di videosorveglianza, i principi, come definiti nel richiamati articoli 5 e 3, di liceità, correttezza, trasparenza, limitazione delle finalità e minimizzazione dei dati, esattezza, limitazione della conservazione, integrità riservatezza e responsabilizzazione.
7. Il Comune di Oliena promuove la sottoscrizione di protocolli di intesa, patti per la sicurezza e patti per l'attuazione, convenzioni o accordi comunque denominati con soggetti pubblici e soggetti privati.

Art. 2 - Definizioni ai sensi dell'Articolo 4 del Regolamento Europeo 2016/679

Ai fini del presente Regolamento si intende:

1. **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

2. **Particolari categorie di dati:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del GDPR).
3. **Dati personali relativi a condanne penali e reati**: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).
4. **Dato anonimo:** il dato che a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
5. **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
6. **Limitazione di trattamento:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
7. **Profilazione:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica,la salute, le preferenze personali, gli interessi, l'affidabilità, il
comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
8. **Pseudonimizzazione:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive 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;
9. **"Blocco":** la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
10. **Titolare:** 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;
11. **DPO - Data Protection Officer:** persona designata dal Titolare o dal Responsabile come centro di competenza per il corretto trattamento dei dati personali.
12. **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratti dati personali per conto del titolare del trattamento.
13. Persone autorizzate al trattamento: le persone fisiche autorizzate, in base a specifiche istruzioni, a compiere operazioni di trattamento dal titolare o dal responsabile.
14. Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
15. Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
16. Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al

trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

17. Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
18. Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
19. Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
20. Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
21. Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro

Art. 3 - Principi generali

1. Ai sensi della vigente normativa in materia di sicurezza urbana i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per tutela della sicurezza urbana, la cui definizione è stata da ultimo riformulata dal dl 14/2017, convertito nella legge 18 aprile 2017 n. 48, all'art. 4 e definita come il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio da potenziare con accordi/patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza. Si riassumono di seguito i principi per il trattamento dei dati che saranno garantiti scrupolosamente:

- **Principio di liceità**: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso, infatti, è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui i comuni e il comando di polizia locale sono investiti.
- **Principio di necessità**: i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati 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.
- **Principio di proporzionalità**: nel commisurare la necessità del sistema di videosorveglianza al 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 una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti.
- **Principio di finalità**: gli scopi perseguiti devono essere determinati, espliciti e legittimi. È consentita la videosorveglianza come misura complementare volta a tutelare la sicurezza urbana anche nell'ambito di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o comunque con lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

Art. 4 Base giuridica del trattamento

1. Il trattamento dei dati personali effettuati tramite il sistema di videosorveglianza può essere considerato lecito solo in quanto necessario per il perseguimento del legittimo interesse del titolare del trattamento per le finalità di cui all'art. 7, valido e prevalente sugli interessi, i diritti e le libertà dell'interessato, ai sensi dell'art. 6, comma 1, lett. f) del Reg. UE 2016/679.
2. L'interesse legittimo predetto deve avere una reale consistenza, dimostrata dal fatto che si sia verificata una situazione di disagio nella vita reale, danni o incidenti gravi in passato. Alla luce del principio di responsabilità, gli incidenti rilevanti si dovrebbero documentare, annotando in un apposito registro la data, le modalità, la perdita finanziaria e le relative accuse penali. Questi incidenti documentati possono rilevare un adeguato interesse legittimo.
3. Nel caso in cui le Forze di Polizia o l'Autorità Giudiziaria richiedano la consegna di alcuni video per lo svolgimento delle indagini, la base giuridica del trattamento deve essere rinvenuta nell'adempimento ad un obbligo di legge a cui è soggetto il Titolare del trattamento, ai sensi dell'art. 6, par. 1, lett. c), del Reg. UE 2016/679.

Art. 5 - Soggetti

1. Titolare per il trattamento dei dati è il Comune di Oliena.
2. Designati al trattamento dei dati rilevati con apparecchi di videosorveglianza sono:
   - □ il Responsabile Comandante della Polizia locale per le telecamere *connesse* alla centrale operativa della Polizia Locale;
   - □ Altri soggetti nominati dall'Ente per le telecamere non connesse alla centrale operativa della Polizia Locale
2. I designati individuano e nominano, con proprio provvedimento, gli autorizzati alla gestione dell'impianto nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio.
3. L'amministratore o gli amministratori di sistema sono designati dal comune.
4. Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.
5. In relazione alle finalità di attuazione di un sistema di sicurezza integrata, di cui al successivo articolo 7 del presente regolamento, poiché finalità e mezzi saranno determinati congiuntamente dagli enti coinvolti, il comune sarà contitolare del trattamento, ai sensi dell'articolo 26 del GDPR nonché articolo 17 della direttiva polizia.

Art. 6 - Informativa

1. Ai sensi dell'art. 13 del Reg. UE 2016/679, il titolare del trattamento deve fornire agli interessati dettagliate informazioni in merito al trattamento dei dati effettuato. Alla luce del volume di informazioni che è necessario fornire all'interessato, è preferibile seguire un approccio a più livelli: le informazioni più importanti dovrebbero essere visualizzate sul cartello di avvertimento stesso (primo livello o informativa semplificata) mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).
2. Le informazioni sul sistema di videosorveglianza possono essere fornite in combinazione con un'icona al fine di fornire, in modo facilmente visibile, comprensibile e chiaramente leggibile, una panoramica significativa del trattamento previsto.

3. Il cartello contenente le informazioni dovrebbe essere posizionato ad una distanza ragionevole dai luoghi monitorati, in modo tale che l'interessato possa facilmente riconoscere l'esistenza della videosorveglianza prima di entrare nell'area monitorata (approssimativamente a livello degli occhi). Non è necessario specificare l'ubicazione precisa delle apparecchiature di sorveglianza, purché non vi siano dubbi su quali aree siano soggette a monitoraggio e sia chiaro in modo inequivocabile il contesto della sorveglianza.
4. L'interessato deve essere in grado di stimare quale area è acquisita da una telecamera in modo da poter evitare la sorveglianza o adattare il suo comportamento, se necessario.
5. I cartelli affissi dovrebbero trasmettere le informazioni più importanti, come:
   a. i dettagli delle finalità del trattamento;
   b. l'identità del Titolare del trattamento;
   c. l'esistenza dei diritti dell'interessato;
   d. le informazioni sui maggiori impatti del trattamento come, ad esempio, gli interessi legittimi perseguiti dal Titolare del trattamento (o da una terza parte) e i dettagli di contatto del Titolare della Protezione dei Dati;
   e. le informazioni più dettagliate di secondo livello, dove e come trovarle;
   f. tutte le informazioni che potrebbero impressionare l'interessato, come la trasmissione dei dati a terzi, in particolare se si trovano al di fuori dell'UE, o il relativo periodo di conservazione. Se queste informazioni non sono indicate, l'interessato dovrebbe presumere che esiste solo un monitoraggio in tempo reale (senza alcuna registrazione o trasmissione di dati a terzi);
   g. dove trovare le ulteriori informazioni sul trattamento dei dati, disponibili in un luogo facilmente accessibile all'interessato tramite fonte digitale (ad esempio QR-code o indirizzo di un sito Web) o analogica (es. banco informazioni).

6. L'informativa completa deve contenere tutti i dati previsi dall'art. 13 del Reg. UE 2016/679 e deve essere messa a disposizione degli interessati con modalità di facile accesso.
7. Tenuto conto del fatto che le riprese potrebbero, seppur in via esclusivamente incidentale, riguardare i dipendenti e collaboratori, il titolare deve mettere a disposizione del personale una copia del presente regolamento e una copia dell'informativa sul trattamento dei propri dati personali, consultabili in qualunque momento anche mediante estrazione di copia.
8. Nel rispetto di quanto previsto dall'art. 4, comma 1, della legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori), prima ancora di procedere all'installazione ed utilizzazione di un sistema di videosorveglianza dal quale possa derivare la possibilità di controllo dei dipendenti, il Titolare deve siglare un accordo con le rappresentanze sindacali per l'installazione dell'impianto (nel caso in cui superi la soglia occupazionale di 15 dipendenti) oppure richiedere l'Autorizzazione all'installazione alla Direzione Territoriale del Lavoro (nel caso in cui la soglia occupazionale non venga superata).
9. Sul sito istituzionale del comune e presso gli uffici individuati è disponibile l'informativa concernente le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal GDPR relativamente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla direttiva polizia relativamente 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.

Art. 7 - Finalità dei sistemi e architettura degli impianti

1. Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite ai comuni. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre polizie locali e delle forze di polizia a competenza generale, dovrà essere specificamente disciplinato con appositi atti, patti e convenzioni.
2. Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:
   - attuazione di un sistema di sicurezza integrata ai sensi dell'art. 2 del dl 14/2017;
   - tutela della sicurezza urbana e della sicurezza pubblica;
   - tutela degli operatori e del patrimonio comunale;
   - tutela della protezione civile e della sanità pubblica;
   - tutela della sicurezza stradale;
   - tutela ambientale e polizia amministrativa;
   - prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali
   - arresto in flagranza differito (Art. 10 co. 6 quater D.L. 14/2017)
   - attuazione di atti amministrativi generali (art. 2-ter Codice privacy novellato dalla legge 205/2021 e art. 5 D. lgs 51/2018)
3. Il sistema di videosorveglianza implica il trattamento di dati personali che possono essere rilevati da telecamere tradizionali eventualmente munite di algoritmi di analisi video, metadatazione, conteggio delle persone e verifica dei comportamenti o varchi lettura targhe connessi a black list o altre banche dati, in grado di verificare la regolarità di un transito di un veicolo.
4. Il comune promuove, per quanto di propria competenza, il coinvolgimento dei privati per la realizzazione di singoli impianti di videosorveglianza, orientati comunque su aree o strade pubbliche o ad uso pubblico, nel rispetto dei principi di cui al presente regolamento, previa valutazione di idoneità dei siti e dei dispositivi, normalmente senza connessioni al sistema centrale e senza possibilità di accesso ai filmati, ma con connessioni preferibilmente stand alone. I privati interessati assumono su di sé ogni onere per acquistare le attrezzature e renderle operative in conformità alle caratteristiche tecniche dell'impianto pubblico, le mettono a disposizione dell'ente a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa. Il comune può assumere su di sé gli oneri per la manutenzione periodica e la responsabilità della gestione dei dati raccolti.
5. Nei casi di cui al comma precedente, in accordo con il comune e previa stipula di apposita convenzione, i soggetti privati che hanno ceduto i propri impianti di videosorveglianza all'ente possono decidere, con oneri a proprio carico, di affidare il controllo in tempo reale delle immagini ad un istituto di vigilanza privato, con il compito di allertare ed interessare in tempo reale le forze di polizia in caso di situazioni anomale.
6. Il comune può dotarsi di body cam, dash cam, droni, telecamere riposizionabili (anche del tipo foto-trappola), altri dispositivi mobili (anche con generazione di allarmi da remoto per il monitoraggio attivo). Le modalità di impiego dei dispositivi in questione saranno stabilite nel disciplinare programma e/o con apposito provvedimento del comando di polizia locale.
7. Nel rispetto delle finalità previste nel presente regolamento, dalle immagini di videosorveglianza potranno essere acquisiti elementi utili alla verbalizzazione di violazioni amministrative, nel rispetto delle vigenti normative e regolamenti.
8. Fermo restando la competenza tecnica dei soggetti interni all'Ente (UTC e amministratore di sistema) e previa una valutazione d'impatto sulla protezione dei dati (DPIA) ogni implementazione del sistema di

videosorveglianza dovrà essere preventivamente asseverato con una deliberazione di Giunta in grado di evidenziare e portare a terra i fondamentali principi del Regolamento UE 2016/679 e del D.lgs. 51/2018 ovvero la rispondenza del proposto intervento ai principi di legalità, proporzionalità, necessità, finalità e minimizzazione del trattamento.

Art. 8 - Trattamento e conservazione dei dati

1. I dati personali oggetto di trattamento effettuato con strumenti elettronici nel rispetto delle misure minime indicate dalla normativa relative alla protezione delle persone fisiche sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per le finalità di cui al precedente art. 7 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;
   d) conservati per le telecamere collegate alla centrale operativa per un periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione. Tale termine potrà essere esteso per finalità di indagine, mediante un ulteriore atto in applicazione della Legge 205/2021. Di tale ulteriore conservazione se ne darà notizia nell'informativa completa ai sensi dell'art. 13 del Reg. UE 2016/679 pubblicata sul sito internet comunale oltre che nel disciplinare-programma;
   e) conservati per le telecamere a tutela del solo patrimonio comunale (o per altre telecamere non collegate alla centrale operativa del corpo) per un periodo non superiore a 72 ore successive alla rilevazione, fatte salve speciali esigenze di sicurezza urbana e sicurezza pubblica.
2. In osservanza degli articoli 32 e 35 GDPR e 23 e 25 della direttiva polizia, il comune redige uno o più appositi atti di valutazione dei rischi e di valutazione di impatto sulla protezione dei dati ed adotta le misure in esse previste.
3. Il Comune ha adottato una specifica procedura per la gestione degli incidenti di sicurezza / data breach che garantisce il rispetto delle disposizioni del Reg. UE 2016/679 e la notifica all'Autorità Garante per la Protezione dei dati personali in caso di violazioni di dati personali.

Art. 9 - Modalità di raccolta dei dati

1. I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di telecamere installate in luoghi pubblici ed aperti al pubblico nonché in immobili di proprietà comunale, ubicati nel territorio di competenza.
2. Le telecamere di cui al precedente comma, finalizzate alla tutela della sicurezza urbana, consentono riprese video anche con utilizzo di algoritmi, possono essere dotate di brandeggio e di zoom ottico e sono collegate alla centrale operativa del comando di polizia locale, che potrà, esclusivamente per il perseguimento dei fini istituzionali, eventualmente digitalizzare o indicizzare le immagini.
3. Le immagini sono conservate per il periodo indicato all'art. 8. Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione, ove tecnicamente possibile, con modalità tali da rendere non più utilizzabili i dati cancellati.

Art. 10 - Diritti dell'interessato

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

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

b) di essere informato sugli estremi identificativi del titolare e del designato al trattamento, oltre che sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali ed in generale di tutto quanto previsto ex art. 13 GDPR e art. 10 e ss. D. lgs 51/2018;

c) di ottenere:

- la conferma dell'esistenza o meno di dati personali che lo riguardano;
- la trasmissione in forma intelligibile dei medesimi dati e della loro origine;
- la cancellazione nei casi previsti dal Regolamento UE 2016/679 qualora sussista uno dei motivi di cui all'art. 17 del GDPR, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

d) di opporsi, nei casi previsti dal Regolamento UE 2016/679, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21 del GDPR. Il designato informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti.

e) di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'art. 18 del GDPR. In tali casi i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico.

2. 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.

3. Le istanze sono presentate al titolare o al designato al trattamento.

Art. 11 - Accesso ai filmati.

1. Al di fuori dei diritti dell'interessato, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente.
2. Ogni richiesta deve essere specifica, formulata per iscritto, motivata ed indirizzata al designato del trattamento dei dati competente entro 3 giorni dall'evento.
3. Non è consentito fornire direttamente ai cittadini copia delle immagini, salvo il rispetto della legge n. 241/90 e delle relative procedure.
4. Per finalità di indagine, l'Autorità giudiziaria e la Polizia giudiziaria possono richiedere ed acquisire copia delle immagini in formato digitale.
5. Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, copia delle riprese in formato digitale può essere richiesta ed acquisita dall'organo di polizia stradale che ha proceduto ai rilievi ed in capo al quale è l'istruttoria relativa all'incidente.
6. Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'art. 391-quater c.p.p., può richiedere ed acquisire copia delle riprese in formato digitale previo pagamento delle

relative spese individuate con apposita deliberazione di giunta comunale sulle tariffe di accesso ai documenti amministrativi.

7. Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere al designato del trattamento che i filmati siano conservati oltre i termini di legge, per essere messi a disposizione dell'organo di polizia procedente. Spetta all'organo di polizia procedente presentare richiesta di acquisizione dei filmati. Tale richiesta deve pervenire entro tre mesi dalla data dell'evento, decorsi i quali i dati non saranno ulteriormente conservati.
8. In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'addetto incaricato dal designato del trattamento dei dati deve annotare le operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, con lo scopo di garantire la genuinità dei dati stessi.

Art. 12 - Persone autorizzate al trattamento

Ai sensi dell'art. 2-quaterdecies del D. Lgs. 196/2003, così come modificato dal d.lgs. 101/2018 e del Reg. UE 2016/679, il titolare del trattamento deve individuare formalmente i soggetti che, all'interno del Comune di Oliena, siano autorizzati ad accedere ai dati raccolti attraverso il sistema di videosorveglianza e, di conseguenza, a visualizzare le immagini.

Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

Tali soggetti, il cui numero deve essere limitato a quanto strettamente necessario, devono essere nominati per iscritto e devono ricevere tutte le istruzioni in merito al corretto utilizzo del sistema.

Tali istruzioni vengono fornite dal fornitore/installatore del sistema ad integrazione del presente regolamento e del Regolamento aziendale per il trattamento dei dati personali, i cui principi devono essere sempre tenuti a mente ed applicati:

1. Le persone autorizzate al trattamento devono accedere ai locali dove sono situate le postazioni di controllo solo ove sia indispensabile per gli scopi perseguiti, con l'obbligo di prestare la massima attenzione al fine di evitare che altri soggetti, anche inavvertitamente, possano prendere visione delle predette immagini.
2. Il monitor dal quale sia possibile visualizzare le immagini deve sempre essere rivolto in modo tale da evitare che gli altri soggetti non autorizzati possano, volontariamente o meno, prendere visione delle immagini.
3. Nessun soggetto non autorizzato al trattamento dei dati deve poter accedere alle aree di controllo del sistema di videosorveglianza. Nel caso in cui queste ultime non siano costantemente presidiate, il dipendente o collaboratore dovrà assicurarsi di mettere in stand-by il monitor e di chiudere a chiave la stanza nella quale sia posizionato il monitor.
4. In nessun caso le immagini acquisite tramite il sistema di videosorveglianza potranno essere utilizzate per scopi di natura personale né per scopi differenti da quelli per i quali i dati sono raccolti.
5. Le registrazioni contenenti i dati personali potranno essere estratte solamente su autorizzazione scritta del Titolare, in seguito a potenziali eventi anomali (furti, danni, intrusioni non autorizzate, malfunzionamenti del sistema, etc) o su richiesta delle Autorità per finalità di indagini di polizia o

giudiziaria. Tali richieste dovranno necessariamente essere formalizzate in forma scritta e conservate, quale evidenza della necessità di accedere i dati.

Tutte le persone autorizzate al trattamento devono attenersi strettamente alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle stesse.
Il mancato rispetto delle predette istruzioni può comportare l'irrogazione di sanzioni disciplinari, oltre che responsabilità di natura civilistica.

Art. 13 - Responsabili esterni del trattamento

Nel caso in cui l'installazione e la successiva gestione del sistema di videosorveglianza vengano effettuati da una società esterna, quest'ultima deve essere preliminarmente nominata Responsabile esterno del trattamento ai sensi dell'art. 28 del Reg. UE 2016/679, in relazione all'ambito di trattamento definito. La predetta nomina, con valenza contrattuale, deve essere redatta in forma scritta e deve contenere le istruzioni in merito al corretto trattamento dei dati personali.
A seguito della sua sottoscrizione, il responsabile è tenuto al rispetto di tutti gli obblighi dettati dall'art. 28 del Reg. UE 2016/679, tra i quali mettere a disposizione del Titolare del trattamento le informazioni necessarie per dimostrare il rispetto degli obblighi normativi e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento.

Art. 14 - Misure di sicurezza tecniche

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
La sicurezza del sistema e dei dati, ovvero la protezione da interferenze intenzionali e non intenzionali durante la normale attività dovrebbe includere:

a. protezione dell'intera infrastruttura di videosorveglianza (comprese telecamere remote, cavi e alimentatore) contro manomissioni fisiche e furti;
b. protezione della trasmissione di filmati con canali di comunicazione sicuri contro l'intercettazione;
c. crittografia dei dati;
d. utilizzo di soluzioni basate su hardware e software come firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;
e. rilevamento di guasti di componenti, software e interconnessioni;
f. mezzi per ripristinare la disponibilità e l'accesso al sistema in caso di incidente fisico o tecnico.

In base alle caratteristiche dei sistemi utilizzati, i soggetti autorizzati al trattamento o, eventualmente, responsabili esterni del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.
Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (controllo dei

log). Il controllo degli accessi garantisce infatti che solo le persone autorizzate possano accedere al sistema e ai dati, mentre viene impedito agli altri di farlo. Le misure che supportano il controllo dell'accesso fisico e logico devono:

a. garantire che tutti i locali in cui viene effettuato il monitoraggio della videosorveglianza e vengono archiviate le riprese video siano protetti contro l'accesso non controllato da parte di terzi;
b. definire ed applicare le procedure per la concessione, la modifica e la revoca dell'accesso fisico e logico;
c. implementare metodi e mezzi di autenticazione e autorizzazione dell'utente, incluso ad esempio la lunghezza delle password e la frequenza di modifica;
d. registrare e rivedere periodicamente le azioni eseguite dall'utente (sia sul sistema che sui dati) tramite il controllo dei log di accesso;
e. effettuare il monitoraggio e il rilevamento degli errori di accesso in modo continuo e affrontare tempestivamente le carenze.

Nel caso in cui il sistema sia configurato per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione.
Nel caso in cui sia necessario effettuare interventi di manutenzione, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini.

Art. 15 - DPIA (Data Protection Impact Assessment)

Ai sensi dell'articolo 35, paragrafo 1, Il Titolare è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) quando un tipo di trattamento dei dati può comportare un rischio elevato per i diritti e la libertà delle persone fisiche e se il trattamento costituisce un monitoraggio sistematico di un'area accessibile al pubblico su larga scala.
Nello specifico, secondo il chiarimento interpretativo fornito dal Garante per la protezione dei dati personali con l'Allegato 1 al Provvedimento n. 467 dell'll ottobre 2018 [doc. web n. 9058979 - Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018 contenente l' Elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto] la valutazione d'impatto è obbligatoria quando "dai trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8)."
Il Titolare del trattamento dei dati dovrebbe quindi effettuare tale valutazione e, sulla base del risultato della DPIA eseguita, dovrebbe determinare la scelta delle misure di protezione dei dati da implementare.
È anche importante notare che se i risultati della DPIA indicano che il trattamento comporta rischi elevati nonostante le misure di sicurezza pianificate dal Titolare del trattamento, sarà necessario prima di iniziare il trattamento consultare l'Autorità di controllo competente.

Art. 16 - Cessazione del trattamento dei dati

In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati

secondo quanto previsto dal GDPR relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, e dall'art 2 della direttiva polizia 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.

Art. 17 - Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 77 e seguenti del GDPR relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, dagli artt. 37 e seguenti della direttiva polizia 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.

2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 46 della legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati personali, così come individuato dal precedente art.5.

Art. 18 - Norma di rinvio

Per quanto non disciplinato dal presente Regolamento si rinvia al D.lgs 51/2018 e al D.lgs 101/2018 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.