

COMUNE DI CERRETO D'ESI

PROVINCIA DI ANCONA

REGOLAMENTO PER LA DISCIPLINA E L'UTILIZZO DEI SISTEMI DI VIDEOSORVEGLIANZA COMUNALE

Approvato con deliberazione di Consiglio Comunale n._ del _____

Indice

REGOLAMENTO PER LA DISCIPLINA E L'UTILIZZO DEI SISTEMI DI VIDEOSORVEGLIANZA COMUNALE	1
TITOLO I – Disposizioni Generali	
Articolo 1 – Oggetto e Normativa di Riferimento.....	2
Articolo 2 – Principi Generali.....	3
Articolo 3 - Definizioni e Soggetti.....	5
Articolo 4 – Valutazione di impatto sulla protezione dei dati.....	8
Articolo 5 – Informativa	8
Articolo 6 – Finalità del trattamento mediante sistemi di videosorveglianza	9
TITOLO II - Sistemi di videosorveglianza	
Articolo 7 - Architettura dei sistemi di videosorveglianza	10
Articolo 8 - Modalità di raccolta dei dati.....	11
Articolo 9 - Trattamento e conservazione dei dati.....	12
Articolo 10 - Sicurezza dei dati	12
Articolo 11 - Data breach	14
Articolo 12 - Cessazione del trattamento dei dati	14
Articolo 13 - Disposizioni in materia di videosorveglianza per finalità particolari	14
TITOLO III - Esercizio dei diritti degli interessati e accesso alle registrazioni	
Articolo 14 - Diritti dell'interessato	17
Articolo 15 - Accesso alle registrazioni	18
TITOLO IV - Comunicazioni e diffusione dei dati	
Articolo 16 – Comunicazione	20
TITOLO V – Disposizioni Finali e Transitorie	
Articolo 17 - Tutela amministrativa e giurisdizionale	20
Articolo 18 - Provvedimenti attuativi	20
Articolo 19 - Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali	20
Articolo 20 - Disposizioni finali.....	21

TITOLO I – Disposizioni Generali

Articolo 1 - Oggetto e normativa di riferimento

1. Il Regolamento per la disciplina dei sistemi di videosorveglianza comunale (da ora anche solo “regolamento”) regola le modalità di trattamento dei dati personali mediante sistemi di videosorveglianza e relativi strumenti e applicativi di gestione nell’ambito del territorio di competenza del Comune di Cerreto d’Esi (da ora anche solo “Comune”), stabilendo altresì norme tecniche e organizzative di dettaglio.
2. Il regolamento concorre a definire la base giuridica, le finalità e le modalità del trattamento, anche ai sensi della Legge 3 Dicembre 2021, N. 205.
3. Il sistema di videosorveglianza finalizzato alla sicurezza pubblica è composto dal complesso di apparecchiature, strumenti, software, dispositivi e ogni altro tipo di tecnologia collegata o comunque connessa ad un centro di controllo, finalizzati alla vigilanza da remoto, ossia a distanza, mediante riprese video. Il sistema può altresì essere integrato, ma non necessariamente connesso, con bodycam, dashcam, telecamere ricollocabili (anche tipo “fototrappola”) e Unmanned Aircraft System (sistemi aeromobili a pilotaggio remoto, c.d. “droni”, in seguito solo “UAS”) e quant’altro la tecnologia metta a disposizione, compresi autovelox, telelaser, tutor, documentatori di infrazioni in area semaforica o connesse all’accesso in ZTL e/o APU, rilevatori di veicoli privi di assicurazione.
4. Le riprese e i fotogrammi, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi la videosorveglianza rileva sul diritto e le libertà delle persone, in ordine alla propria riservatezza.
5. Con il regolamento si garantisce che il trattamento dei dati personali, effettuato mediante l’impiego di sistemi di videosorveglianza come sopra definito, gestiti dal Comune nell’ambito della propria attività istituzionale, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza personale. Sono altresì garantiti 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.
6. Il regolamento per la disciplina dei sistemi di videosorveglianza è adottato nel rispetto dei principi e con riferimento ai seguenti provvedimenti normativi e comunicati ufficiali da parte del Garante Privacy;
 - a) Regolamento UE 2016/679, 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)”;
 - b) Decreto legislativo 30 Giugno 2003, N. 196 e s.m.i., recante “Codice in materia di protezione dei dati personali”;
 - c) Decreto legislativo 10 Agosto 2018, N. 101, recante “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) 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 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”;

e) Decreto legislativo 18 Maggio 2018, N. 51, recante “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”;

f) Legge 3 Dicembre 2021, N. 205, recante “Conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali”;

g) Linee guida n.3/2019 del 29 gennaio 2020 emesse dal Comitato europeo per la protezione dei dati;

h) Regolamento comunale per la tutela della riservatezza rispetto al trattamento dei dati personali e successiva approvazione delle disposizioni organizzative per l’attuazione della normativa in materia di trattamento dei dati personali. (Reg.UE 2016/679).

i) Garante Privacy, comunicato e nota 14-11-2022: Videosorveglianza: stop del Garante privacy a tecnologie riconoscimento facciale e occhiali smart da Pa e lavoratori.

7. Il regolamento in particolare, ai sensi dell’articolo 5 del Regolamento UE 2016/679 e articolo 3 della Direttiva UE 2016/680, stabilisce le norme di dettaglio finalizzate all’attuazione, con riguardo ai trattamenti dei dati personali effettuati mediante l’uso di sistemi di videosorveglianza, dei principi, di liceità, correttezza, trasparenza, limitazione delle finalità e minimizzazione dei dati, esattezza, limitazione della conservazione, integrità riservatezza e responsabilizzazione.

8. Possono essere sottoscritti protocolli di intesa, patti per la sicurezza e patti per l’attuazione, convenzioni o accordi, comunque denominati, con soggetti pubblici e soggetti privati, al fine di implementare e condividere sistemi di videosorveglianza per la tutela della sicurezza urbana di cui all’articolo 6 del presente regolamento.

Articolo 2 - Principi generali

1. Il trattamento dei dati personali attraverso il sistema di videosorveglianza avviene secondo i principi generali di:

a) responsabilizzazione (accountability)

- nel fornire una garanzia di completa accessibilità alle informazioni che riguardano i cittadini in quanto utenti del servizio (principio di trasparenza);
- nella capacità effettiva di rendere conto delle scelte fatte, dei comportamenti, delle azioni attuate e di rispondere alle questioni poste dai portatori di interessi generali (principio della responsabilità);

- nella capacità effettiva di fare rispettare le norme sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori (principio della conformità);

b) protezione dei dati fin dalla progettazione (privacy by design) ovvero la necessità di tutelare i dati personali sin dalla fase di sviluppo, progettazione, selezione di un progetto che comporti l'utilizzo di applicazioni, servizi e prodotti per il trattamento di dati personali, creando sistemi che sin dall'inizio dell'attività limitino possibili violazioni dei dati raccolti (articolo 25 comma 1 del GDPR);

c) protezione dei dati per impostazione predefinita (privacy by default) ovvero la necessità di implementare misure giuridiche, tecniche e organizzative efficaci e adeguate a garantire che siano trattati solo i dati personali necessari per ciascuna finalità specifica del trattamento, con l'impostazione a priori della massima protezione dei dati attraverso il loro minimo trattamento sia in fase di raccolta sia in fase di trattamento successivo all'acquisizione, secondo i principi di necessità e pertinenza (articolo 25 comma 2 del GDPR).

2. La videosorveglianza è principalmente finalizzata alla tutela della Sicurezza Urbana, come da ultimo formulata dal Decreto legge 20 Febbraio 2017, N. 14, convertito con Legge 18 Aprile 2017, N. 48 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.

3. Si riassumono di seguito i principi per il trattamento dei dati che saranno garantiti nella gestione di sistemi di videosorveglianza comunale:

a) 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.

b) 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.

c) 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.

d) 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.

4. L'uso dei dati personali nell'ambito di cui trattasi, non necessita del consenso degli interessati, in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate alla normativa vigente in materia di protezione dei dati personali.

Articolo 3 – Definizioni e Soggetti

1. Ai fini del presente regolamento si intende:

a) Per “**banca dati**”, il complesso di dati personali acquisiti, trattato mediante riprese video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;

b) Per “**trattamento**”, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

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

d) Per “**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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

e) Per “**responsabile**”, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

f) Per “**autorizzati**”, coloro che sono definiti “**designati**” e “**incaricati**” che agiscono sotto l'autorità del Titolare o del responsabile e che possono gestire dati personali per le funzioni che gli competono;

g) Per “**designati**”, coloro che operano sotto l'autorità del Titolare o del responsabile del trattamento e sono stati individuati da questi per svolgere compiti e funzioni connessi al trattamento di dati relativi al sistema di videosorveglianza;

h) Per “**incaricati**” coloro che operano sotto l'autorità del Titolare o del responsabile del trattamento e che, a seguito di nomina, anche da parte del Designato, svolgono attività di trattamento dei dati personali in relazione al sistema di videosorveglianza;

i) Per “**interessato**”, la persona fisica, cui si riferiscono i dati personali trattati;

- l) Per “**comunicazione**”, l’operazione di portare a conoscenza a uno o a più soggetti determinati, diversi dall’interessato, in qualunque forma, anche mediante la messa a disposizione o consultazione dei dati personali afferenti l’interessato;
- m) Per “**diffusione**”, l’operazione di dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- n) Per “**dato anonimo**”, il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- o) Per “**blocco**”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
- p) Per “**brandeggio**”, il supporto per telecamera che può ruotare contemporaneamente in senso orizzontale e verticale;
- q) Per “**terzo**”, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- r) Per “**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;
- s) Per “**responsabile della protezione dei dati**”: soggetto designato dall’Ente, con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali;
- t) Per “**DPIA**”: acronimo di “Data Protection Impact Assessment”, è la procedura di valutazione d’impatto della protezione dei dati personali, ai sensi dell’art. 35, comma 3, lettera c) del GDPR;

2. **Il Titolare per il trattamento dei dati è il Comune di Cerreto d’Esi** a cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali.

3. **I Designati al trattamento** sono le persone fisiche, legate da rapporto di servizio al Titolare e preposto dal medesimo al trattamento di dati personali al quale il Titolare stesso demanda alcune responsabilità previste nel presente Regolamento. Possono essere designati al trattamento dei dati rilevati con apparecchi di videosorveglianza i soggetti che, per esperienza, capacità ed affidabilità, forniscono le garanzie previste dalle predette norme di cui all’art. 1. Salvo diversa indicazione, designati al trattamento dei dati rilevati con apparecchi di videosorveglianza sono:

- a) il Comandante della Polizia locale per le telecamere collegate o comunque connesse alla centrale operativa, nonché le bodycam, dashcam, telecamere ricollocabili (anche tipo “fotrappola”) e UAS (c.d. droni) e quant’altro la tecnologia metta a disposizione, compresi autovelox, telelaser, tutor, documentatori di infrazioni in area semaforica o connesse all’accesso in ZTL e/o APU, rilevatori di veicoli privi di assicurazione;

- b) gli altri Dirigenti/Responsabili dei Settori/Unità di Staff e/o di Progetto competenti per le telecamere a tutela del patrimonio comunale o, comunque non collegate alla centrale operativa della Polizia locale.
4. Tali designati vengono puntualmente individuati con atto del Comune, che impartisce direttive e fornisce istruzioni per la gestione ottimale del trattamento di dati mediante videosorveglianza.
 5. I Titolari ed i Responsabili individuano e nominano, con proprio provvedimento, gli autorizzati alla gestione dell'impianto e al trattamento dei dati nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio e secondo le effettive esigenze operative, determinando profili specifici di autorizzazione al trattamento.
 6. Gli autorizzati al trattamento dei dati e alla gestione degli impianti sono le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dai designati al trattamento.
 7. L'amministratore o gli amministratori dei sistemi sono figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e alle quali è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione. L'amministratore o gli amministratori dei sistemi sono designati dal titolare del trattamento.
 8. Con l'atto di nomina ai singoli autorizzati sono affidati i compiti specifici e le puntuali istruzioni e prescrizioni per l'utilizzo dei sistemi di Videosorveglianza.
 9. **Il Responsabile del trattamento** (la cui individuazione, nomina e disciplina è contenuta all'articolo 28 del Regolamento europeo 2016/679 e, laddove applicabile, nell'articolo 18 del Decreto legislativo 18 maggio 2018, n. 51), è la persona fisica e giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Qualora, per esigenze connesse alle operazioni di gestione dei dati, o qualsiasi altra attività che comporti l'accesso ai dati per l'esercizio dei sistemi di videosorveglianza, si dovesse rendere necessario ricorrere a responsabili del trattamento esterni all'Amministrazione comunale, che svolgono il trattamento per conto del titolare, questi devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi la conformità alla normativa vigente e garantisca la tutela dei diritti dell'interessato.
 10. In ogni caso, la nomina di soggetti esterni all'Amministrazione comunale deve avvenire secondo le vigenti disposizioni organizzative per l'attuazione della normativa in materia di trattamento dei dati personali del Comune di Cerreto d'Esi.
 11. In relazione alle finalità di attuazione di un sistema di sicurezza integrata, di cui all'articolo 6 del presente regolamento, poiché le finalità e mezzi saranno determinati congiuntamente dagli Enti coinvolti, il Comune sarà contitolare del trattamento, ai sensi dell'articolo 26 del Regolamento UE 2016/679, nonché articolo 17 della Direttiva 2016/680.
 12. Il titolare del trattamento è tenuto a designare il Responsabile della Protezione dei Dati, a norma dell'articolo 37 del Regolamento UE 2016/679 e dell'articolo 28 del Decreto legislativo 18 Maggio 2018, N. 51. La nomina del Responsabile della Protezione dei Dati, esterno all'Amministrazione comunale, deve avvenire secondo le vigenti Disposizioni

organizzative per l'attuazione della normativa in materia di trattamento dei dati personali del Comune di Cerreto d'Esi.

13. Per le ulteriori definizioni si rinvia a quanto previsto dall'art. 4 del Regolamento UE 2016/679 e, laddove applicabile, nell'articolo 2 del Decreto legislativo 18 maggio 2018, N. 51.

Articolo 4 - Valutazione di impatto sulla protezione dei dati

1. A norma dell'articolo 35, commi 1 e 3, lettera c) del Regolamento UE 2016/679, il trattamento di dati mediante sistemi di videosorveglianza, in ragione delle tecnologie impiegate e della predisposizione alla sorveglianza sistematica su larga scala di una zona accessibile al pubblico, è soggetto alla valutazione di impatto sulla protezione dei dati personali da parte del titolare.
2. Laddove ricorrano i presupposti, la valutazione di impatto sulla protezione dei dati personali deve essere effettuata anche a norma dell'articolo 23 del Decreto legislativo 18 Maggio 2018, N. 51.
3. L'insieme di trattamenti simili svolti mediante sistemi di videosorveglianza, può essere esaminato con una singola valutazione. Qualora si ritenga comunque opportuno, può darsi corso a valutazioni separate per ciascun trattamento.
4. La valutazione di impatto sulla protezione dei dati personali è redatta dal Titolare del trattamento, anche con ausilio di soggetti incaricati quali esperti, dotati di specifiche conoscenze e competenze tecnico-giuridiche, avvalendosi della consulenza del responsabile per la protezione dei dati personali.
5. La valutazione di impatto sulla protezione dei dati personali è adottata secondo le vigenti Disposizioni organizzative per l'attuazione della normativa in materia di trattamento dei dati personali del Comune di Cerreto d'Esi.

Articolo 5 - Informativa

1. I soggetti interessati che stanno per accedere o che si trovino in una zona videosorvegliata devono essere informati mediante apposita segnaletica che costituisce informativa di primo livello, o ridotta, nei casi specificamente previsti dalla normativa vigente.
2. La segnaletica di cui al comma precedente è realizzata conformemente alla normativa vigente.
3. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, possono essere installati più cartelli, o comunque con modalità tali da rendere possibile a tutti i soggetti che accedono all'area di essere informati della presenza dei dispositivi di videoripresa.
4. Sul sito web istituzionale del Comune e presso gli uffici competenti è disponibile l'informativa concernente le finalità del sistema di videosorveglianza, le modalità di raccolta e conservazione dei dati, le modalità di diritto di accesso dell'interessato secondo quanto previsto dal Regolamento UE 2016/679 e dalla Direttiva 2016/680.

Articolo 6 - Finalità del trattamento mediante sistemi di videosorveglianza

1. Le finalità a cui sono dirette l'installazione e l'impiego degli impianti di videosorveglianza sono quelle istituzionali demandate al Comune di Cerreto d'Esi, così come indicate dal provvedimento dell'Autorità Garante in materia di videosorveglianza dell'8 aprile 2010 e successive integrazioni, modifiche o aggiornamenti, dal D.Lgs. 18 agosto 2000 n. 267, nonché dallo Statuto Comunale e dai Regolamenti Comunali vigenti. In particolare, le predette sono riconducibili al controllo del territorio e alla prevenzione e razionalizzazione delle azioni contro gli illeciti penali ed amministrativi nell'ambito delle misure di promozione e attuazione del sistema di sicurezza urbana per il benessere della comunità locale.

Il trattamento dei dati personali mediante sistemi di videosorveglianza è principalmente effettuato ai fini di:

- a) tutela della sicurezza urbana e della sicurezza pubblica;
- b) tutela degli operatori e del patrimonio comunale;
- c) protezione civile e sanità pubblica;
- d) tutela della sicurezza stradale;
- e) tutela ambientale e polizia amministrativa;
- f) prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali;
- g) rilevare e accertare violazioni al codice della strada a mezzo di dispositivi elettronici e/o automatici;
- h) altre attività connesse.

2. Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

3. L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.

La localizzazione delle telecamere e le modalità di ripresa saranno sempre determinate in ossequio ai richiamati principi.

4. La possibilità di avere a disposizione dati ed immagini costituisce uno strumento di prevenzione e di razionalizzazione dei compiti che la Polizia Locale svolge quotidianamente nell'ambito delle proprie competenze istituzionali; attraverso tali strumenti si perseguono finalità di tutela della popolazione e del patrimonio comunale nonché del patrimonio ambientale e culturale, garantendo quindi un elevato grado di sicurezza nei luoghi di maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.

5. L'uso dei dati personali nell'ambito definito dal presente Regolamento, non necessita del consenso degli interessati in quanto viene effettuato per l'esecuzione di un compito di interesse

pubblico o comunque connesso all'esercizio di pubblici poteri e allo svolgimento di funzioni istituzionali di cui è investito il Comune.

6. I sistemi di videosorveglianza di cui al presente regolamento, non possono essere impiegati per l'accertamento differito e la notificazione di sanzioni per violazioni amministrative alle norme del Codice della Strada, al di fuori dei casi espressamente consentiti dallo stesso Codice della Strada. È in ogni caso consentito l'utilizzo dei sistemi di videosorveglianza e delle registrazioni, nell'ambito dell'accertamento di violazioni amministrative a norma dell'articolo 13 della Legge 24 Novembre 1981, N. 689.

7. L'impiego del sistema di videosorveglianza per finalità di tutela della sicurezza pubblica e protezione civile, e di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con accesso anche sistematico da parte delle forze di Polizia dello Stato e o da parte di altre Polizie Locali, dovrà essere disciplinato con appositi atti, patti e convenzioni.

TITOLO II - Sistemi di videosorveglianza

Articolo 7 - Architettura dei sistemi di videosorveglianza

1. I sistemi di videosorveglianza prevedono il trattamento di dati personali che possono essere rilevati da telecamere, anche munite di algoritmi di analisi video, di metadatazione, di conteggio delle persone e verifica dei comportamenti, o dispositivi di "lettura targhe" interfacciati con "black-list" o altre banche dati, in grado di verificare la regolarità di un transito di un veicolo.
2. 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.
3. Il Comune per tutelare la sicurezza urbana nonché favorire la sicurezza integrata di cui al Decreto Legge 14/2017 convertito nella Legge 18 aprile 2017, n. 48 "Disposizioni urgenti in materia di sicurezza delle città" può destinare il sistema di videosorveglianza comunale per la tutela della sicurezza urbana con finalità interforze; pertanto l'utilizzo andrà specificamente disciplinato ed organizzato.
4. Il sistema di videosorveglianza, in relazione alle esigenze della Polizia locale, può essere integrato, ma non necessariamente connesso, con bodycam, dashcam, UAS, telecamere ricollocabili (anche 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 con apposito provvedimento del Comandante del Servizio di Polizia Locale. Il personale addetto riceverà apposito disciplinare tecnico sull'utilizzo delle bodycam, delle dashcam e degli UAS, nonché l'informativa sul trattamento dei loro dati personali che indirettamente potrebbero essere trattati in relazione all'evolversi degli scenari che fanno insorgere situazioni di pericolo, turbamento dell'ordine e della sicurezza pubblica e nel caso di pericolo imminente per persone e/o cose o di insorgenza di situazioni di criticità.

5. 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.
6. Fermo restando la competenza tecnica del CPOSP (Comitato di Ordine e Sicurezza Provinciale) e dell'UTG (Ufficio Territoriale di Governo) ogni implementazione del sistema di videosorveglianza dovrà essere preventivamente approvata con una delibera di Giunta che evidenzii il rispetto dei principi fondamentali del Regolamento UE 2016/679 e del Decreto Legislativo 51/2018 ovvero la rispondenza del proposto intervento ai principi di legalità, proporzionalità, necessità, finalità e minimizzazione del trattamento.
7. Compete alla Giunta Municipale l'individuazione delle zone ritenute maggiormente sensibili e dei siti da sottoporre a videosorveglianza. Ogni nuova installazione di sistemi di videosorveglianza dovrà essere vagliata, sentito preliminarmente il Comandante della Polizia Locale. Con deliberazione di Giunta Municipale sono elencati gli impianti di videosorveglianza attivati nel territorio del Comune di Cerreto d'Esi, la loro ubicazione (per quelli fissi) e le loro principali caratteristiche. Analoga deliberazione dovrà essere adottata per modificare o integrare gli impianti di videosorveglianza.
8. E' fatta salva la possibilità per il Comandante della Polizia Locale di individuare altri siti strategici temporanei, per le finalità proprie del presente regolamento.

Articolo 8 - Modalità di raccolta dei dati

1. I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di telecamere che inquadrano luoghi pubblici e aperti al pubblico, nonché in immobili di proprietà comunale, ubicati nel territorio di competenza.
2. L'attività di videosorveglianza deve raccogliere solo dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando solo immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.
3. Le telecamere installate nel Comune di Cerreto d'Esi, consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.
4. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato.
5. I segnali video delle unità di ripresa saranno inviati presso l'Unità di ricezione, registrazione e visione ubicata nell'Ufficio Polizia Locale. In questa sede le immagini saranno visualizzate su monitor e registrate su supporto magnetico.
6. Le telecamere di cui ai precedenti commi, finalizzate alla tutela della sicurezza urbana, consentono riprese video anche con utilizzo di algoritmi di analisi, possono essere dotate di brandeggio e di zoom ottico, con le limitazioni pertinenti al caso rispettando i principi di liceità e limitazione dei dati e sono collegate alla centrale operativa del Servizio di Polizia locale, che potrà, esclusivamente per il perseguimento dei fini istituzionali, digitalizzare o indicizzare le immagini.

7. L'utilizzo del brandeggio (movimento di rotazione di bracci mobili di strumenti o apparecchiature) e dello zoom da parte del Designato e degli autorizzati al trattamento deve essere conforme alle finalità dell'impianto riportate all'articolo 6 del presente Regolamento.

8. Le immagini videoregistrate sono conservate per il periodo indicato nell'articolo 9 della presente informativa. Decorso il termine di conservazione il sistema di videoregistrazione provvede in automatico alla loro cancellazione, ove tecnicamente possibile, mediante sovra registrazione, con modalità tali da rendere non più utilizzabili i dati cancellati.

Articolo 9 - Trattamento e conservazione dei dati

1. I dati personali oggetto di trattamento effettuato mediante sistemi di videosorveglianza, 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 articolo 6 e resi utilizzabili per operazioni compatibili con esse;

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

d) conservati, per quanto riguarda i dati raccolti mediante le telecamere collegate alla centrale operativa, per un periodo ordinariamente non superiore a sette giorni successivi alla rilevazione, che può essere esteso tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati. Termini specifici di conservazione dei dati in relazione alle singole finalità sono eventualmente individuati dalla Legge e specificamente esaminati nella valutazione di impatto sulla protezione dei dati di cui all'articolo 4;

e) conservati per le telecamere a tutela del solo patrimonio comunale (o per altre telecamere non collegate alla centrale operativa del Servizio di Polizia Locale o comunque non gestite da operatori di Polizia locale) per un periodo non superiore a 72 ore successive alla rilevazione, fatte salve speciali esigenze di sicurezza urbana e sicurezza pubblica.

f) trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, con modalità volta a salvaguardare l'anonimato.

Articolo 10 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati presso la centrale di registrazione, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite dal designato al trattamento dei dati.

2. In particolare, la centrale di registrazione delle telecamere del sistema di videosorveglianza finalizzato alla sicurezza cittadina, collegate o comunque connesse alla centrale operativa della Polizia Locale, è ubicata presso la sede della Polizia Locale, in specifico locale, il cui accesso è riservato al personale abilitato mediante sistema di identificazione individuale. I flussi video delle telecamere di campo sono trasmessi in via prioritaria mediante rete in fibra ottica dedicata;

residualmente in modalità wireless, in modalità crittografata. I dati raccolti sono inviati a server destinati esclusivamente alla videosorveglianza.

Mediante quest'ultimi, le immagini sono rinviate alle postazioni di controllo. I flussi video sono registrati su Network Video Recorder dedicato unicamente alla videosorveglianza. L'infrastruttura logica di rete locale non è in condivisione con altre infrastrutture di rete comunale.

3. In particolare, l'accesso agli ambienti in cui è ubicata una postazione di controllo è consentito solamente al personale autorizzato e per scopi connessi alle finalità previste nonché alle società incaricate alla manutenzione degli impianti debitamente nominate Responsabili del trattamento, alla pulizia dei locali e per occasionali motivi istituzionali. L'accesso è comunque soggetto ad autorizzazione da parte del titolare o del designato al trattamento.

4. Il designato impartisce idonee istruzioni atte ad evitare assunzioni o rilevamenti abusivi di dati, da parte dei soggetti terzi che accedono ai locali.

5. La gestione e l'utilizzo dei sistemi di videosorveglianza aventi finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è riservata agli organi di polizia locale ed alle forze di polizia a competenza generale, aventi qualifica di ufficiali ed agenti di polizia giudiziaria ai sensi dell'articolo 57 del codice di procedura penale.

6. Il Responsabile del trattamento individua e nomina gli autorizzati in numero sufficiente a garantire l'efficace e efficiente gestione del servizio di videosorveglianza.

7. Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.

8. In ogni caso, prima dell'utilizzo degli impianti, essi sono istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento, del presente regolamento e degli ulteriori provvedimenti adottati.

9. Gli autorizzati al trattamento sono dotati di proprie credenziali di autenticazione al sistema.

10. Il sistema deve essere fornito di dati di "log" relative all'accesso e alle operazioni eseguite da ciascun utente, le cui informazioni dovranno essere conservate per la durata di almeno sei mesi.

11. I sistemi di registrazione e conservazione dei dati devono essere configurati in modo da non permettere accessi diretti alle cartelle e ai file, mantengano almeno per 6 mesi le registrazioni (log) di tutte le attività effettuate dagli utilizzatori (di qualsiasi livello, utente o amministratore di sistema).

12. In caso di prolungato inutilizzo dell'account (per più di 6 mesi), in caso di cessazione o trasferimento degli incaricati autorizzati, è necessario che manualmente o tramite specifiche policy automatiche si provveda alla disabilitazione delle credenziali di accesso. L'eventuale riabilitazione dovrà essere autorizzata dal Responsabile del trattamento.

13. I supporti, sui quali sono registrati o esportati i dati acquisiti mediante l'utilizzo dell'impianto di videoregistrazione, sono conservati, a cura del Designato, in luogo idoneo posto nella disponibilità del Servizio di Polizia Locale.

14. In caso di sostituzione dei supporti di registrazione (hard disk), quelli in disuso devono essere distrutti con modalità tali da renderne impossibile il recupero dei dati conservati (wipe-out).

15. Il Titolare o il Responsabile del trattamento impartiscono istruzioni organizzative e tecniche per la custodia e l'uso di eventuali supporti rimovibili, su cui siano memorizzati i dati, al fine di evitare accessi non autorizzati e trattamenti non consentiti.

Articolo 11 - Data breach

1. Una violazione di sicurezza o data-breach sulle registrazioni video è un evento che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati avvenuto in modo accidentale o in modo illecito.

2. Ai sensi di quanto stabilito dal GDPR (art. 33 Reg. UE 2016/679), in caso di data breach è necessario seguire la prevista procedura che prevede tra l'altro, nei casi più gravi, la comunicazione all'Autorità Garante entro 72 ore dal momento in cui se ne è avuta conoscenza.

3. In tutti i casi è necessario avvertire il Designato e in particolare il DPO che provvederanno a documentare l'avvenuta violazione nel registro dei data breach.

Articolo 12 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati secondo quanto previsto dal Regolamento Ue 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, e dall'articolo 2 del Decreto Legislativo 51/2018 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Articolo 13 - Disposizioni in materia di videosorveglianza per finalità particolari

1. Nei casi in cui la videosorveglianza sia attivata presso istituti scolastici di competenza comunale, il sistema installato, nel rispetto di quanto previsto dall'Autorità Garante, deve garantire il diritto dello studente alla riservatezza, prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione.

2. In tale quadro, può risultare ammissibile l'utilizzo di tali sistemi, in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree esterne e soltanto negli orari di chiusura degli istituti.

3. È vietato la ripresa di eventuali attività extrascolastiche all'interno della scuola.

4. Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non pertinenti o private.

5. La videosorveglianza attivata per finalità di controllo deposito/abbandono rifiuti e tutela ambientale (cd. fototrappole o altri analoghi strumenti di controllo puntuale), in applicazione dei richiamati principi di minimizzazione, limitazione delle finalità e proporzionalità, effettuata con dispositivi fissi e/o mobili, è consentito nei seguenti casi:

- a) con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo/improprio di aree pubbliche, o aperte al pubblico, impiegate come discariche di materiali e/o di sostanze pericolose;
- b) con riferimento alle attività di controllo, in aree pubbliche o aperte al pubblico, volte ad accertare il corretto rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti;
- c) con riferimento alle attività di controllo e verifica del rispetto delle norme a tutela dell'ambiente e del territorio, consentendo di rilevare e accertare le infrazioni a norma di legge di regolamento ed alle ordinanze Comunali, quando non risulti possibile, o si rilevi non efficace, il ricorso a strumenti e sistemi di controllo alternativi.

6. Il sistema delle "fototrappole" comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese e che, in relazione ai luoghi di installazione dei suddetti strumenti, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.

7. Al fine di prevenire e reprimere gli illeciti ambientali derivanti dall'inosservanza di specifiche leggi in materia (Testo Unico Ambientale – D. Lgs. 152/2006 e ss.mm.ii.) e gli illeciti amministrativi e/o penali derivanti dalle violazioni alle disposizioni di legge e di regolamento, emanate anche con riferimento alle modalità di conferimento dei rifiuti e del ciclo R.S.U., l'Amministrazione si avvale del sistema di videosorveglianza comunale localizzando le telecamere in siti considerati critici e di particolare interesse, nei quali le classiche misure di controllo del territorio non siano risultate sufficienti e/o inadatte ad ottenere oggettivi risultati.

Le risultanze fotografiche individuano unicamente gli elementi indispensabili per la redazione del verbale di accertamento delle violazioni amministrative e sanzioni accessorie, laddove previste, secondo quanto previsto dalla vigente normativa. Le stesse immagini non vengono inviate di norma al domicilio del contravventore, ferma restando l'accessibilità da parte degli aventi diritto. La documentazione video- fotografica è resa disponibile a richiesta dell'intestatario del verbale, al momento dell'accesso vengono in ogni caso oscurati o resi comunque non riconoscibili persone o elementi non pertinenti alla violazione.

I dati rilevati sono accessibili anche per fini di Polizia Giudiziaria e di Pubblica Sicurezza, per la prevenzione o l'accertamento di eventuali reati. In questo caso, sono fatte salve le esigenze di ulteriore conservazione dei dati come derivanti da una specifica richiesta investigativa o dell'Autorità Giudiziaria, anche in relazione ai procedimenti e/o alle indagini in corso.

8. La videosorveglianza per i sistemi di monitoraggio del traffico e/o rilevazione delle violazioni (autovelox, telelaser, tutor, documentatori di infrazioni in area semaforica o connesse all'accesso in ZTL e/o APU, rilevatori di veicoli privi di assicurazione) comporta il trattamento di dati personali rilevati mediante le riprese e che riguardano i mezzi di trasporto che transitano nelle aree sottoposte agli impianti e, in base alle condizioni generali di inquadratura, l'immagine degli interessati. Le registrazioni sono immediatamente scartate nel caso di assenza di violazione delle norme del codice della strada mentre sono conservate per i connessi provvedimenti sanzionatori.

In conformità al provvedimento del Garante per la protezione dei dati personali 8 aprile 2010:

- a) gli impianti elettronici di rilevamento circoscriveranno la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;

b) le risultanze fotografiche e/o le riprese video potranno individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (ad esempio, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta). Pertanto, sarà effettuata una ripresa del veicolo che non comprenda o, in via subordinata, schermi, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (ad esempio, pedoni, soggetti trasportati, altri utenti della strada);

c) le risultanze fotografiche e/o le riprese video rilevate saranno utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale. Ferma restando la loro accessibilità da parte degli aventi diritto, nei soli casi previsti, all'occorrenza sarà data informazione al soggetto interessato della detenzione agli atti delle immagini (o delle riprese video) quali elementi di prova da utilizzate per l'accertamento della violazione;

d) le immagini saranno conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione dell'illecito, all'eventuale applicazione di una sanzione pecuniaria e/o accessoria, alla riscossione anche coattiva e alla definizione del possibile contenzioso in conformità alla normativa di settore. Sono fatte salve eventuali esigenze di ulteriore conservazione, derivanti da una specifica richiesta investigativa dell'Autorità Giudiziaria o di Polizia Giudiziaria, in materia penale;

e) le fotografie e/o le immagini che costituiscono elemento di prova per le violazioni contestate, di norma, non saranno inviate d'ufficio all'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;

f) la visione della documentazione video-fotografica sarà resa disponibile a richiesta del destinatario del verbale di accertamento, nei modi, tempi e forme previsti. Al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo o elementi non pertinenti alla violazione.

9. Sono in ogni caso obbligatorie le informazioni indicate al precedente art.5 della presente informativa.

10. Ai sensi di quanto previsto dall'articolo 4 della Legge 20 maggio 1970 n. 300 e s.m.i., gli impianti di videosorveglianza non possono essere utilizzati per effettuare controlli sull'attività lavorativa dei dipendenti dell'Ente, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

11. L'utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso anche da parte delle forze di polizia a competenza generale, dovrà essere specificamente disciplinato con appositi atti.

Sarà possibile anche allestire una centrale operativa interforze dove ogni operatore di polizia locale o dello Stato, debitamente autorizzato, qualificato e tracciato potrà accedere ed operare nel rispetto delle proprie diverse prerogative.

In tali casi gli accordi tra le parti dovranno garantire il rispetto del presente Regolamento ed i diritti degli interessati.

TITOLO III - Esercizio dei diritti degli interessati e accesso alle registrazioni

Articolo 14 - Diritti dell'interessato

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

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

b) di essere informato sugli estremi identificativi del titolare del trattamento, oltre che sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali ed in generale di tutto quanto previsto dall'articolo 13 del Regolamento Ue 2016/679 e articolo 10 e Decreto Legislativo 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;
- l'informazione sulle procedure adottate in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento;
- la cancellazione nei casi previsti dal Regolamento UE 2016/679 qualora sussista uno dei motivi di cui all'articolo 17 del Regolamento Ue 2016/679, 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;
- 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'articolo 21 del Regolamento Ue 2016/679. Il Titolare del trattamento informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti;
- di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'articolo 18 del Regolamento Ue 2016/679. 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. Nell'esercizio dei diritti di cui al comma 1, l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi.

4. Nel caso in cui le istanze non siano adeguatamente riscontrate, l'interessato ha la facoltà di inoltrare una segnalazione all'Autorità Garante per protezione dei dati personali.

Articolo 15 - Accesso alle registrazioni

1. Al di fuori dei diritti dell'interessato, l'accesso alle registrazioni della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente.

2. L'accesso alle immagini è consentito esclusivamente:

a) al Titolare, al Responsabile del trattamento ed agli incaricati del trattamento;

b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);

c) alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo ovvero, in casi del tutto eccezionali, all'amministratore informatico del sistema comunale (preventivamente individuato quale incaricato del trattamento dei dati);

d) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta. L'accesso da parte dell'interessato, sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte del Soggetto Designato del trattamento, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;

3. Ogni richiesta deve essere specifica, formulata per iscritto, motivata e indirizzata al Titolare, al Responsabile del trattamento dei dati entro 72 ore dall'evento.

Per accedere ai dati ed alle immagini registrate, l'interessato dovrà presentare un'apposita istanza scritta ed adeguatamente motivata, corredata obbligatoriamente, a pena di improcedibilità, dalla fotocopia del proprio documento di identità e contenente obbligatoriamente un recapito digitale di posta elettronica e/o posta elettronica certificata per ricevere le comunicazioni attinenti al procedimento.

Le successive comunicazioni trasmesse dal Comune agli indirizzi e-mail o p.e.c. indicati obbligatoriamente dal soggetto istante nella propria domanda, si intendono valide e pienamente conosciute ad ogni effetto di legge.

L'istanza di cui al comma 3, preferibilmente trasmessa all'Ente in forma telematica, deve altresì indicare precisamente a quale sito dell'impianto di videosorveglianza si fa riferimento, nonché il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di video-ripresa.

Nel caso di accertamento negativo, ovvero in cui le indicazioni rese dall'istante siano assenti e/o inconferenti e/o insufficienti a permettere il reperimento delle immagini registrate, o in mancanza dell'attestazione del contributo di spesa assolto, se e come previsto, sarà data comunicazione al richiedente circa l'improcedibilità della stessa, così come nell'ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione per avvenuta decorrenza del termine e/o comunque indisponibili all'accesso nei casi previsti dalla legge e/o per qualsiasi altra motivazione. In caso di mancata allegazione della fotocopia del documento di identità e del recapito digitale di posta elettronica e/o posta elettronica certificata all'istanza presentata, la stessa si considera d'ufficio direttamente improcedibile.

In relazione all'istanza pervenuta, verificata la procedibilità delle medesima, l'Ufficio preposto sarà tenuto ad accertare l'effettiva esistenza delle immagini richieste e di ciò si darà comunicazione al richiedente, di norma entro i cinque giorni successivi al ricevimento della domanda, e nel caso di accertamento positivo entro i successivi 15 giorni, fisserà e comunicherà altresì la data e l'ora in cui il suddetto richiedente potrà accedere alle immagini che lo riguardano e l'Ufficio comunale presso il quale presentarsi per il ritiro di eventuale documentazione.

L'accesso alle riprese da parte dell'interessato non può in ogni caso estendersi ai dati personali di soggetti terzi. Ove non sia possibile separare i dati personali del richiedente da quelli di soggetti terzi, ciò dovrà essere oggetto di distinta e specifica ponderazione dell'Ufficio preposto ai fini della procedibilità o delle eventuali tutele aggiuntive da adottarsi per il caso concreto.

4. Il diritto di accesso, di cui alla Legge 7 Agosto 1990 n. 241, non può essere esercitato per acquisire le immagini riprese dalle telecamere di video sorveglianza. È fatto salvo, nel rispetto delle vigenti normative speciali, il diritto di accesso ai documenti amministrativi derivanti dalla visione delle immagini da parte degli organi di polizia.

5. Per finalità di indagine, l'Autorità giudiziaria e la polizia giudiziaria possono richiedere e acquisire copia delle registrazioni in formato digitale.

6. Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, copia delle riprese in formato digitale può essere richiesta e acquisita dall'organo di polizia stradale che ha proceduto ai rilievi e in capo al quale è l'istruttoria relativa all'incidente.

7. Salvo il caso si tratti di documenti già acquisiti dall'Autorità giudiziaria, nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'art. 391-quater c.p.p., può richiedere e acquisire copia delle riprese in formato digitale.

8. 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 cui all'articolo 9 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 sei mesi dalla data dell'evento, decorsi i quali i dati non saranno ulteriormente conservati.

9. In ogni caso di accoglimento delle richieste di accesso di cui al presente articolo, l'Ufficio preposto dovrà curare affinché siano annotate le operazioni eseguite al fine di acquisire i filmati e/o il riversamento su documentazione cartacea o supporto digitale, con lo scopo di garantire la trasparenza delle attività e la genuinità dei dati stessi.

10. Possono comunque essere divulgate immagini provenienti dagli impianti di videosorveglianza, previa anonimizzazione di ogni dato che consenta l'identificazione dei soggetti.

11. La consegna della copia delle riprese in formato digitale prevede il pagamento delle relative spese, individuate con apposita deliberazione di Giunta comunale riguardante le tariffe di accesso ai documenti amministrativi.

12. In relazione al trattamento dei dati personali, è assicurato agli interessati il diritto a richiedere al Titolare del trattamento l'accesso ai propri dati, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o la possibilità di opporsi al trattamento, nei casi previsti dalla legge, facendo valere questi e gli altri diritti previsti dal G.D.P.R. e ss.mm.ii. tramite comunicazione scritta e motivata, fatta pervenire al Titolare del trattamento.

TITOLO IV - Comunicazioni e diffusione dei dati

Articolo 16 - Comunicazione

1. La comunicazione dei dati personali da parte del Comune di Cerreto d'Esi a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o da regolamento e/o convenzione. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria ed esclusivamente per lo svolgimento delle funzioni istituzionali.
2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone autorizzate per iscritto a compiere le operazioni del trattamento dal Titolare o dal Designato.
3. È in ogni caso fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del Codice Privacy per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.
4. In via eccezionale, possono essere diffuse immagini o foto, riprese con il sistema di videosorveglianza, esclusivamente previa autorizzazione da parte dell'Autorità Giudiziaria, per finalità di prevenzione, accertamento o repressione di reati o per la ricerca di persone scomparse.

TITOLO V – Disposizioni Finali e Transitorie

Articolo 17 - Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli articoli. 77 e seguenti del Regolamento Ue 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, dagli articoli. 37 e seguenti del Decreto Legislativo 51/2018 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 articoli 4-6 della Legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati personali, così come individuato dal precedente articolo 3 della suddetta informativa.

Articolo 18 - Provvedimenti attuativi

1. Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi conseguenti al presente Regolamento, in particolare la predisposizione dell'elenco dei siti di ripresa nonché la definizione di ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento.

Articolo 19 - Diritto al risarcimento, responsabilità e danni cagionati per effetto del trattamento di dati personali

1. Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal Soggetto Designato del trattamento ai sensi delle disposizioni di cui all'art. 82, RGPD.
2. Il titolare o il Soggetto Designato del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
3. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2, RGPD.

Articolo 20 - Disposizioni Finali

1. Copia del presente Regolamento sarà pubblicata all'albo pretorio e potrà essere reperita sul sito internet del Comune <https://www.comune.cerretodesi.an.it>.
2. Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.
3. Il presente regolamento abroga ogni disposizione regolamentare precedente che disciplina tale materia.
4. Per quanto non espressamente disciplinato dal presente Regolamento, si rinvia al Reg. UE 2016/679 (GDPR), al D. Lgs 51/2018 e al Codice Privacy novellato (d.lgs. 196/2003 e s.m.i.), al provvedimento in materia di videosorveglianza emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010 e le linee guida EDPB, aggiornate il 28 marzo 2023 con l'adozione formale delle linee guida 09/2022 dell'EDPB, nonché alle altre disposizioni normative vigenti in materia.