Regolamento comunale per la protezione dei dati personali e del sistema di videosorveglianza

TITOLO I

NORME INTRODUTTIVE

ART. 1 - Oggetto

1. Il presente Regolamento disciplina le misure procedimentali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia nell'attuazione:

a) del Regolamento UE n. 2016/679 del 27 aprile 2016 (di seguito "GDPR") e del "Codice in materia di protezione dei dati personali" approvato con D.Lgs. 30 giugno 2003, n.196, di seguito denominato "Codice" come modificato dal D.Lgs 101 del 10 agosto 2018;

b) della Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio e del Decreto Legislativo 18 maggio 2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali", nonché alla libera circolazione di tali dati;

In particolare:

a) disciplina il trattamento dei dati personali effettuato dal Comune nello svolgimento dei propri compiti istituzionali;

b) individua i compiti del Titolare e dei Responsabili, nonché degli Autorizzati del trattamento dei dati personali esistenti e gestiti presso gli uffici comunali;

c) disciplina le modalità di raccolta, trattamento e conservazione dei dati personali mediante sistemi di videosorveglianza gestiti dal Comune di Capannori nell'ambito dei propri immobili e/o del proprio territorio.

ART. 2 - Definizioni

1. Ai fini del presente Regolamento si intende per:

- Titolare del trattamento: il Comune di Capannori quale entità organizzativa complessa, e per essa il legale rappresentante, il Sindaco;
- Responsabile : soggetto delegato che esercita le funzioni del Titolare: i singoli Dirigenti del Comune ed i Responsabili di UOA (Unità Organizzativa Autonoma) per i rispettivi ambiti di competenza ovvero, in ragione delle specificità organizzative della struttura di appartenenza;
- Autorizzati: i soggetti interni autorizzati per competenza da parte del Responsabile;
- Responsabile esterno del trattamento: la persona fisica o giuridica, o altro organismo, estraneo al Comune di Capannori, che tratta dati personali per conto del titolare del trattamento;
- Responsabile della protezione dei dati (RPD): il soggetto che svolge i compiti di cui all'art. 39 del GDPR o gli ulteriori compiti affidati dal titolare del trattamento.

2. Per le altre definizioni si rinvia all'art. 4 GDPR.

ART. 3 - Finalità del trattamento

1. I trattamenti sono compiuti dal Comune per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;

b) l'adempimento di un obbligo legale al quale è soggetto il Comune;

c) l'esecuzione di un contratto con soggetti interessati o per la conclusione dello stesso;

d) per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;

e) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

2. Rientrano nelle finalità di cui al comma 1 lett. a) i trattamenti compiuti per:

a) l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;

b) la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;

c) l’esercizio di ulteriori funzioni amministrative affidate al Comune per servizi di competenza statale o regionale in base alla vigente legislazione, ovvero per altri servizi in base a convenzione;

d) la tutela in giudizio del Comune;

e) la promozione e l’attuazione del sistema di sicurezza urbana per il benessere della comunità locale.

TITOLO II

ORGANIZZAZIONE DEL TITOLARE

ART. 4 - Titolare del trattamento

1. Il Comune di Capannori è il Titolare del trattamento dei dati personali compiuto per lo svolgimento delle relative funzioni istituzionali dalle proprie articolazioni organizzative o da parte di terzi per suo conto.

2. Il Titolare definisce, fin dalla fase di progettazione, le necessarie misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato in modo conforme al GDPR e al Codice.

3. Gli interventi necessari per l’attuazione delle misure di cui al precedente comma sono inseriti nell’ambito degli strumenti di programmazione.

4. Le funzioni di Titolare del trattamento sono esercitate da ciascun Responsabile nel rispettivo ambito di competenza, in conformità all’assetto organizzativo del Comune di Capannori e alle disposizioni del presente regolamento.

ART. 5 - Compiti del Responsabile

1. I Responsabili, nell’ambito delle strutture organizzative cui sono preposti, assicurano il rispetto degli obblighi normativi previsti in capo al Titolare del trattamento in relazione ai trattamenti di loro competenza.

2. Tali soggetti provvedono in particolare a:

a) censire e monitorare costantemente le singole attività di trattamento dei dati personali facenti capo al Settore/UOA

b) eseguire prontamente ogni elemento necessario alla regolare tenuta del Registro unico delle attività di trattamento predisposto dal Comune di Capannori ai sensi dell'art. 11 del presente Regolamento al fine di mantenere costantemente aggiornato lo stesso;

c) designare con atto scritto gli autorizzati al trattamento dei dati personali con le modalità di cui all’art. 9 del presente regolamento;

d) vigilare sulle attività dei soggetti autorizzati di cui al precedente punto e garantire una adeguata formazione nell'ambito delle iniziative predisposte dall'Ente e dal RPD;

e) disciplinare il rapporto con il Responsabile esterno del trattamento e procedere per iscritto alla sua nomina secondo le modalità previste dall'art 8 del presente regolamento;

f) prima di procedere al trattamento, effettuare l'analisi del rischio e, ove necessario, la valutazione di impatto ai sensi dell'art. 35 del GDPR e dell'art. 17 del presente regolamento, in collaborazione con il RPD;

g) provvedere, in relazione alla natura dei dati e alle specifiche caratteristiche del trattamento, a monitorare l'adeguatezza delle misure di sicurezza adottate;

h) notificare al Garante la violazione dei dati personali (data breach) e provvedere alla comunicazione della violazione agli interessati dandone informativa alla Segreteria Generale e al RPD ai sensi dell'art. 18 del presente regolamento;

i) collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

j) garantire l'esercizio dei diritti degli interessati previsti agli articoli da 15 a 18 e da 20 a 22 del GDPR e dar corso alle relative richieste;

k) predisporre le informative in collaborazione con il RPD e curarne il costante aggiornamento;

Art. 6 - Compiti di coordinamento dei Settori

1. Alla Segreteria Generale compete l'adozione delle misure volte a garantire l'uniformità di applicazione del GDPR all'interno dell'ente. Essa svolge attività amministrativa in materia di privacy e fornisce adeguato supporto ai Settori.

2. La Segreteria Generale dispone le modalità operative per la tenuta e aggiornamento del Registro unico dei trattamenti di cui all'art. 11 del presente regolamento e ne pubblica periodicamente gli aggiornamenti. Spetta a ciascun Settore invece l'inserimento tempestivo delle procedure afferenti alle proprie competenze.

3. Ciascun Settore predispone l'elenco degli autorizzati al trattamento che condivide con la Segreteria Generale e lo aggiorna periodicamente;

4. Ciascun Settore nomina uno o più "referenti privacy" per la gestione degli adempimenti connessi alla protezione dei dati, nonché come punto di contatto con il RPD e la Segreteria Generale.

5. La Segreteria Generale collabora e fornisce adeguato supporto al RPD.

6. Le funzioni previste da questo articolo possono essere attribuite a uffici diversi dalla Segreteria Generale attraverso la semplice modifica della macrostruttura e del funzionigramma, senza variare questa disposizione.

ART 7 - Compiti dell'Ufficio Progetti strategici, Innovazione, transizione al digitale

1. All'Ufficio Progetti strategici, Innovazione, transizione al digitale competono lo sviluppo e la gestione delle ,, applicazioni e dei sistemi informatici dell'Ente. Nello svolgimento di tali attività, all'Ufficio Sistemi Informativi spettano i seguenti compiti:

a) provvedere, in relazione alle conoscenze acquisite in base al processo tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, ad adottare e ad aggiornare le idonee e preventive misure di sicurezza per i dati informatici in relazione ai trattamenti di diretta competenza ed a collaborare con gli altri Dirigenti dell'Ente per la definizione delle misure di sicurezza inerenti i trattamenti di competenza degli stessi;

b) programmare e realizzare gli interventi in materia di sicurezza informatica;

c) impartire ai Dirigenti le necessarie istruzioni operative per la sicurezza delle banche dati;

d) curare il coordinamento delle operazioni relative alla sicurezza delle categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR oggetto di trattamento con modalità informatica, provvedendo a prevenire i rischi di distruzione o perdita, anche accidentale;

e) fornire supporto ai Dirigenti, sui profili informatici, per lo svolgimento della Valutazione di impatto di cui all'art. 35 del GDPR.

2. Le funzioni previste da questo articolo possono essere attribuite a uffici diversi da quello Progetti strategici, Innovazione, transizione al digitale attraverso la semplice modifica della macrostruttura e del funzionigramma, senza variare questa disposizione.

Art. 8 - Responsabile esterno del trattamento

1. Il Responsabile nomina quali responsabili esterni del trattamento i soggetti pubblici o privati affidatari, per conto del Comune, di attività e servizi che per la loro realizzazione rendono necessario il trattamento di dati personali o i soggetti terzi che trattano dati sulla base di specifiche convenzioni.

2. Il Responsabile provvede a dare adeguate istruzioni per i trattamenti nel contratto di affidamento o con separato atto giuridico che definisca la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati oltre agli obblighi che il Responsabile si impegna a rispettare con la sottoscrizione.

3. I Responsabili esterni del trattamento sono nominati tra soggetti che forniscono le garanzie di cui all'art. 28 par. 1 GDPR. La sussistenza di tali garanzie deve essere espressamente dichiarata.

ART. 9 - Autorizzati al trattamento

1. Il Responsabile procede a designare, all'interno della propria struttura operativa, il personale dipendente autorizzato per l'espletamento di tutte le operazioni di trattamento dei dati.

2. La designazione è fatta con atto scritto nel quale sono specificati i compiti affidati agli autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.

3. Gli Autorizzati effettuano tutte le operazioni di trattamento dei dati nel rispetto delle istruzioni e direttive impartite dal proprio Responsabile, che prevedono di:

a) accedere solo ai dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;

b) trattare i dati personali di cui si viene a conoscenza per l'espletamento delle proprie funzioni, in modo lecito e corretto, nel rispetto delle norme di legge, dello Statuto e dei Regolamenti che disciplinano le attività del Comune;

c) verificare costantemente i dati, il loro aggiornamento, la loro completezza e pertinenza;

d) custodire con cura atti e documenti contenenti dati personali ricevuti in consegna per adempiere ai compiti assegnati e restituirli al termine delle operazioni affidate;

e) comunicare i dati personali trattati solo previa autorizzazione;

f) osservare scrupolosamente le misure di sicurezza predisposte;

g) osservare, anche in seguito a modifica, trasferimento e/o cessazione del rapporto di lavoro gli obblighi relativi alla riservatezza e alla comunicazione.

ART. 10 - Responsabile della protezione dei dati

1. Il Responsabile della protezione dei dati (RPD) è individuato, con decreto di nomina del Sindaco, che ne stabilisce la durata dell'incarico, fra soggetti in possesso dei requisiti previsti dal GDPR.

2. Il RPD assolve i compiti previsti dall'art. 39 del GDPR e gli eventuali altri compiti affidati alla stesso dal Titolare.

3. Il Comune garantisce al RPD, per l'esecuzione di compiti ad esso affidati, l'autonomia e le risorse necessarie per assolverli.

4. Gli uffici formulano le proprie richieste al RPD dandone contestualmente conoscenza alla Segreteria Generale. Il RPD rende noti i risultati della propria attività consultiva con verbali periodici indirizzati alla Segreteria Generale.

6. Il RPD può convocare incontri con i dirigenti e i dipendenti per l'esecuzione dei propri compiti di informazione, consulenza, sorveglianza e consultazione e può altresì organizzare specifiche giornate di formazione.

7. Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

TITOLO III

TRATTAMENTO DEI DATI PERSONALI

Art. 11 - Registro delle attività di trattamento

1. Il Comune di Capannori tiene un registro Unico dei trattamenti contenente le informazioni di cui all' art. 30 del GDPR che elenca i trattamenti di tutti i settori, pubblicato in Amministrazione trasparente, Altri contenuti, Registro delle attività di trattamento.

2. Ciascun Responsabile è tenuto a redigere ed aggiornare tempestivamente (ogni volta che si presenti la necessità) il Registro delle attività di trattamento svolte nell'ambito della propria competenza.

3. in caso durante l'anno non si verifichino necessità di aggiornamento, dovrà comunque essere effettuata almeno una verifica annuale con registrazione della data nel registro.

ART. 12 - Consenso dell'interessato.

1. Il Comune, in quanto soggetto pubblico non deve chiedere il consenso dell'interessato al trattamento dei dati personali, purché il trattamento medesimo sia conforme ai fini istituzionali dell'Ente di cui all'art.3 del presente regolamento.

2. Nei limitati casi in cui il consenso vada richiesto questo deve essere libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto.

ART. 13 - Informativa

1. L'interessato deve essere preventivamente informato, oralmente o per iscritto, secondo quanto previsto dagli artt. 13 e 14 GDPR.

2. L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice.

3. Nell'informativa devono essere comunicati anche i dati di contatto del Responsabile che effettua il trattamento.

4. Ciascun Responsabile è tenuto ad aggiornare periodicamente le informative utilizzate.

5. L’informativa può essere resa disponibile, oltre che sul sito web del Comune, anche negli uffici mediante affissione.

ART. 14 - Diritti dell’interessato

1. Per l'esercizio dei diritti di cui agli articoli da 15 a 22 GDPR l'interessato presenta richiesta al Responsabile competente al trattamento.

2. Se il trattamento è effettuato da soggetti terzi per conto del Comune, la richiesta viene presentata al Responsabile che ha provveduto alla nomina del Responsabile esterno del trattamento.

3. La richiesta può essere inoltrata anche per posta elettronica.

4. L'esercizio dei diritti dell’interessato è gratuito. Il rilascio di copie non è soggetto a rimborsi di diritti di riproduzione e di ricerca.

5. L'Ufficio competente provvede senza ritardo sulla richiesta, e comunque entro trenta giorni dal suo ricevimento. Se le operazioni necessarie per il riscontro alla richiesta sono complesse o ricorre altro giustificato motivo, il termine per il riscontro è di sessanta giorni.

6. Sono fatte salve le limitazioni di cui agli artt. 2-undecies e 2-duodecis del D.Lgs. 196/2003 e le altre limitazioni previste dalla legge.

7. Di norma si procede alla cancellazione dei dati personali in conformità alle norme sulla conservazione della documentazione amministrativa.

ART. 15 - Sicurezza del trattamento

1. Ciascun Responsabile mette in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio e procede, secondo una pianificazione concordata con il RPD, ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati.

2. Il Comune favorisce l’adesione ai codici di comportamento per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto.

ART 16 - Durata del trattamento

1. Fatto salvo quanto specificamente disposto da disposizioni di settore, la durata del trattamento dei dati personali coincide, di norma, con i tempi di conservazione indicati, in riferimento alle diverse tipologie documentali, nel Manuale di gestione

documentale dell'Ente (Piano di conservazione). La durata dei trattamenti è indicata anche nel Registro Unico di cui all'art. 11.

ART. 17 - Valutazione di impatto

1. Ciascun Responsabile valuta la necessità di sottoporre a valutazione di impatto i trattamenti da effettuare e/o le proprie banche dati; qualora decida di procedere a valutazione di impatto si coordina con il RPD per programmarne le modalità operative.

ART.18 - Violazione dei dati personali (Data Breach)

1. Chiunque venga a conoscenza di una violazione dei dati personali (data breach) è tenuto a segnalarlo al Responsabile che deve provvedere tempestivamente ai sensi del presente articolo.

2. Il Responsabile, ove possibile, notifica la violazione dei dati personali al Garante della protezione dei dati personali entro 72 ore dal momento in cui ne sia venuto a conoscenza, a meno che sia improbabile che la stessa violazione presenti un rischio per la tutela dei diritti e delle libertà delle persone fisiche.

3. La notifica viene effettuata, prevedendo almeno gli elementi indicati al paragrafo 3 dell'articolo 33 del GDPR. La notifica al Garante della protezione dei dati personali effettuata oltre le 72 ore deve essere motivata.

5. Le segnalazioni e le notifiche dei casi di violazione dei dati personali sono comunicati tempestivamente dai Responsabili alla Segreteria Generale e al RPD.

6. Ciascun Responsabile deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza per poter dimostrare il rispetto delle disposizioni del GDPR.

ART. 19 - Formazione del personale

1. Il Comune di Capannori assicura la programmazione e l'organizzazione delle attività formative del personale per la corretta applicazione delle disposizioni in materia di trattamento dei dati personali anche sulla base delle indicazioni e la collaborazione del RPD.

ART. 20 - Trattamento dei dati personali da parte di Amministratori locali

1. Gli Amministratori locali sono legittimati al trattamento dei dati personali esclusivamente nell'esercizio delle proprie funzioni istituzionali e sono tenuti alla riservatezza; in tale esercizio devono assicurare il rispetto del GDPR.

2. I trattamenti dei dati personali effettuati negli Uffici di supporto agli organi politici devono essere svolti da personale adeguatamente informato, formato e autorizzato.

ART. 21 - Comunicazione e diffusione dei dati personali comuni.

1. La comunicazione dei dati personali all'interno dell'Ente per lo svolgimento delle funzioni istituzionali non è soggetta a limitazioni, salvo quelle espressamente previste da leggi e regolamenti.

2. Il Responsabile, valutato il caso, può decidere di adottare le misure necessarie alla tutela della riservatezza degli interessati.

3. La comunicazione dei dati personali ad altri soggetti pubblici e la loro diffusione è disciplinata dall'art. 2 ter del Codice.

TITOLO IV

SISTEMA DI VIDEOSORVEGLIANZA COMUNALE

ART. 22 – Videosorveglianza

1. Per videosorveglianza si intende quel complesso di strumenti finalizzati alla vigilanza in remoto, cioè che si realizza a distanza mediante dispositivi per le riprese video collegati a un centro di controllo e coordinamento. 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. 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 di Capannori si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

ART. 23 – Finalità degli impianti di videosorveglianza

1. Nell'ambito delle proprie finalità istituzionali, il Comune di Capannori impiega i sistemi di videosorveglianza quale strumento di primaria importanza per il controllo del territorio e per la 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.

2. I sistemi di videosorveglianza sono finalizzati:

a) alla tutela dell'ordine e della Sicurezza Pubblica, nella sua declinazione locale di sicurezza urbana, con particolare riguardo alla quiete pubblica e alla civile convivenza;

b) alla prevenzione e contrasto di atti delittuosi, attività illecite ed episodi di microcriminalità diffusa e predatoria commessi sul territorio comunale;

c) alla prevenzione di fenomeni che comportano turbativa del libero utilizzo degli spazi pubblici;

d) al controllo di determinati luoghi del territorio comunale, ritenuti meritevoli di particolare tutela;

e) alla sorveglianza diretta di aree che, in situazioni contingenti, possono presentare elementi di particolare criticità, in concomitanza con eventi rilevanti per l'ordine e la sicurezza pubblica;

f) alla tutela degli immobili o delle opere di proprietà o in gestione del Comune;

g) alla tutela del corretto svolgimento delle attività amministrative del Comune;

h) al monitoraggio dei flussi di traffico veicolare e alle attività rivolte alla sicurezza stradale;

i) al supporto nei controlli e alla raccolta delle evidenze documentali per finalità di polizia amministrativa e ambientale;

j) al supporto operativo in operazioni di protezione civile;

k) alla rilevazione e accertamento di violazioni al Codice della Strada a mezzo di dispositivi elettronici e/o automatici

l) all'adempimento di norme specifiche che prevedono l'utilizzo di sistemi di videosorveglianza.

3. Gli impianti di ripresa di immagini per finalità diverse da quelle elencate nel presente articolo quali la promozione turistica del territorio, le rilevazioni meteorologiche o climatiche, il monitoraggio tecnico di impianti, il monitoraggio di frane o caratteristiche geologiche del territorio o altre finalità, non rientrano nell'ambito del presente regolamento. Tali impianti soggiacciono comunque alla relativa disciplina normativa e all'applicazione del GDPR, fatti salvi i casi in cui le riprese costituiscano dati anonimi, ovvero non permettono l'identificazione diretta o diretta di interessati in conseguenza di angoli di ripresa, definizione e lunghezza focale non sufficiente.

4. Ogni impianto di videosorveglianza oggetto del presente regolamento dovrà essere specificatamente declinato nella sua o nelle sue finalità, sulla base della quale soggiacerà alla relativa disciplina normativa.

ART. 24 – La videosorveglianza e la tutela dei lavoratori

1. Gli impianti di videosorveglianza di cui al presente regolamento sono utilizzati, qualora ne ricorrano i presupposti e, in particolare, nell'ambito della finalità descritta alla lettera f), comma 2, art.23, nel rispetto di quanto stabilito dall'art. 4 della Legge 20 maggio 1970, n. 300.

2. In particolare, quando dall’installazione dei suddetti impianti derivi anche l’ipotetica possibilità di controllo a distanza dell'attività dei lavoratori, l’impiego avviene esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, e l’installazione è preceduta dall’attivazione della procedura con le rappresentanze dei dipendenti o, in mancanza di accordo sindacale, dall’autorizzazione pubblica dell’Ispettorato del lavoro territorialmente competente.

3. Per quanto riguarda le garanzie a tutela dei lavoratori, si specifica:

a) che le apparecchiature riprendono i luoghi di lavoro connessi alle esigenze per le quali viene richiesta la presente autorizzazione;

b) che le telecamere non riprendono luoghi riservati esclusivamente ai lavoratori (a titolo esemplificativo e non esaustivo, spogliatoi o servizi);

c) che le telecamere non effettuano registrazioni audio;

d) ove possibile, le telecamere non riprendono postazioni di lavoro in maniera continuativa;

e) che le immagini non sono in alcun modo diffuse all’esterno, tranne che per la citata necessità di tempestiva consegna all’Autorità giudiziaria competente qualora si verifichi una fattispecie delittuosa;

f) che si provvede ad informare tutti i lavoratori nelle forme previste dall'art.4, comma 3, della legge n. 300/1970;

g) che viene rispettata la disciplina dettata dal Regolamento UE 2016/679 in materia di trattamento dei dati personali

4. Per quanto riguarda le misure di sicurezza presenti nell’impianto, si specifica:

a) che, conformemente all’art. 5 del GDPR, tutti i sistemi di videosorveglianza sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite;

b) che l’accesso agli impianti è sottoposto a specifiche limitazioni e controlli ed è consentito solo al personale espressamente autorizzato. L’accesso ai dati dei sistemi è consentito ai soli soggetti autorizzati (di cui l’elenco è costantemente manutenuto e aggiornato), muniti di credenziali di accesso valide e strettamente personali, che permettono un livello di operatività conforme al profilo di autorizzazione;

c) che l’accesso alle immagini registrate viene tracciato per un congruo periodo non inferiore a 6 mesi tramite apposite funzionalità che consentano la conservazione dei log di accesso;

d) che le registrazioni dei sistemi di videosorveglianza sono conservate con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati e cancellati o anonimizzati una volta decorso tale termine. Per la finalità di cui al presente articolo, i tempi di

conservazione sono individuati in 72 ore, decorsi i quali i dati registrati sono cancellati per mezzo di modalità automatiche;

e) che la cartellonistica che indica la presenza dell'impianto di videosorveglianza è collocato prima del raggio di azione della telecamera, avere un formato ed una posizione tale da essere visibile in ogni condizione ambientale, includere un simbolo di esplicita e immediata comprensione.

f) che viene rispettata la disciplina dettata dal Regolamento UE 2016/679 in materia di trattamento dei dati personali.

g) per quanto compatibili, si applicano le altre disposizioni del presente Regolamento.

Art. 25 - La videosorveglianza per la sicurezza integrata

1. I trattamenti effettuati nell'ambito del presente articolo, rientrano nella disciplina normativa dettata dal D.lgs. 51/2018, sulla base dei principi stabiliti dal Regolamento UE 2016/680. Le finalità dei sistemi integrati rientrano in quelle definite all'art. 23, comma 2 lett. a), b), del presente Regolamento.

2. Per scopi di sicurezza integrata, fermo restando le specifiche competenze e funzioni istituzionali e nei limiti fissati dalle norme vigenti, il trattamento dei dati raccolti mediante il sistema di videosorveglianza comunale è effettuato dalla Polizia Municipale presso la centrale operativa del Comando. È effettuato, altresì, presso le sedi dagli Organi di Polizia di Stato e delle altre Forze di Polizia abilitati alla interconnessione sulla base di specifici accordi e/o progetti diretti a regolare i rapporti di collaborazione interforze.

3. La pianificazione degli impianti di videosorveglianza cittadina inseriti nell'ambito del sistema di sicurezza integrata è realizzata anche in sinergia con gli Enti del territorio e il Comitato Provinciale per l'Ordine e la Sicurezza Pubblica. Il trattamento dei dati effettuato ai sensi e per gli effetti delle disposizioni in materia di sistema di sicurezza integrato è realizzato previa definizione di ruoli e responsabilità di tutti i soggetti a diverso titolo coinvolti, per le finalità determinate che si intende perseguire e la loro gestione operativa, coerentemente con la normativa in materia di protezione dei dati personali.

4. L'Ente aderisce a protocolli o a Patti per l'attuazione della sicurezza urbana con gli altri Enti e soggetti del territorio anche per quanto concerne la gestione della videosorveglianza. In ogni caso, sia nel caso di una gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini dei sistemi di videosorveglianza di altri soggetti, anziché nel diverso caso di gestione unica di un soggetto a ciò preposto, il Comune tratta le immagini esclusivamente nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali.

ART. 26 – Informazioni rese agli interessati

1. Nelle aree in cui sono installate le telecamere, è posizionata un’adeguata e apposita segnaletica sulla quale devono essere riportate le informazioni minime previste dalla normativa nazionale ed europea in vigore in materia. La segnaletica dovrà essere collocata, ove possibile, prima del raggio di azione delle telecamere e nelle sue immediate vicinanze con un formato e un posizionamento tali da renderla chiaramente visibile agli interessati. In presenza di più telecamere, in relazione alla vastità dell’area e alle modalità delle riprese, possono essere installati più cartelli con modalità tali da rendere possibile a tutti i soggetti che accedono all’area di essere informati della presenza dei dispositivi di videoripresa.

2. Sul sito istituzionale dell’Ente sono pubblicate le informative complete contenenti gli elementi previsti dal GDPR e dal Decreto Legislativo 18 maggio 2018, n. 51, compresi il dettaglio delle finalità perseguite in relazione ai sistemi di videosorveglianza in uso, gli eventuali destinatari dei dati raccolti, il periodo o i criteri per determinare il periodo di conservazione dei dati in relazione alle relative finalità, i diritti esercitabili dagli interessati e la modalità di esercizio.

3. Sul sito istituzionale dell’Ente è pubblicato inoltre l’elenco e la collocazione dei sistemi di ripresa fissi con l’indicazione delle caratteristiche e delle finalità perseguite, nonché le ulteriori informazioni ritenute utili alla trasparenza del trattamento e all'esercizio dei diritti da parte degli interessati.

4. Le informative di cui sopra possono essere omesse per particolari installazioni solo per esigenze investigative o particolari di sicurezza pubblica, documentate per iscritto.

ART. 27 – Caratteristiche degli impianti e metodologia di rilevazione

1. I sistemi di videosorveglianza oggetto del presente regolamento comprendono sistemi composti da una o più fotocamere o telecamere, fisse o mobili, in grado di riprendere e registrare immagini e, ove applicabile, suoni, eventualmente supportati da sistemi software di interpretazione delle immagini quali sistemi OCR di lettura automatica delle targhe dei veicoli.

3. I sistemi utilizzati prevedono come regola generale la registrazione delle immagini e la conservazione delle stesse con le regole definite al successivo articolo 31. Ove necessario, in relazione alla finalità perseguita, è consentita la visualizzazione in tempo reale delle immagini tramite monitor presenti presso il Centro operativo, nel rispetto delle autorizzazioni al trattamento dati ricevute. L’accesso può avvenire anche ricorrendo a terminali mobili, debitamente configurati anche con riferimento al profilo della sicurezza della trasmissione

4. Ove necessario per la finalità perseguita e per la limitazione delle immagini registrate dagli impianti di videosorveglianza, l’attivazione delle registrazioni può anche essere associata a sensori di rilevazione movimento che attivano le riprese o a sistemi di notifica o allarme automatico.

5. Per le finalità previste dall’articolo 23 lettera k) del presente regolamento, la Polizia Municipale può utilizzare sistemi di videosorveglianza preposti al rilevamento automatico delle infrazioni al Codice della strada quali misuratori di velocità

(autovelox fissi e mobili), impianti di controllo semaforici, sistemi di controllo stradale a distanza (*Street control*) e varchi di controllo dei veicoli per zone a traffico limitato. Tali sistemi sono soggetti alle modalità di utilizzo previste dalla normativa vigente e alle relative autorizzazioni o indicazioni ministeriali.

6. Per specifiche esigenze volte al raggiungimento delle finalità di cui art. 23 del presente regolamento, il Comune può attivare l'utilizzo di ulteriori sistemi di videosorveglianza veicolati da personale o mezzi della Polizia Municipale quali dispositivi a pilotaggio remoto (*droni*), telecamere indossabili (*body cam*), dispositivi a bordo dei mezzi (*dash cam*). L'adozione di tali sistemi è soggetta a una analisi preventiva che ne stabilisca la necessità e l'efficacia, anche rispetto alla valutazione di strumenti e sistemi di controllo alternativi, in relazione alle finalità previste dal presente regolamento e la conformità normativa, al rispetto del principio di minimizzazione dei dati, alla redazione di uno specifico disciplinare d'uso da parte della Giunta comunale, a una specifica valutazione di impatto ai sensi dell'art. 35 del GDPR e alla formazione degli operatori addetti all'utilizzo degli stessi.

7. L'individuazione dei luoghi da sottoporre a videosorveglianza per finalità di sicurezza urbana, la loro modifica, variazione o cessazione, nel rispetto delle finalità previste dal presente regolamento, compete alla Giunta Comunale che, anche su indicazione del Comandante della Polizia Municipale, identifica le aree sensibili ai fini della sicurezza urbana e del controllo del territorio, con apposita deliberazione, sentita l'Autorità di Pubblica Sicurezza, e condivise le risultanze periodicamente emergenti dal Comitato Provinciale per l'Ordine e la Sicurezza Pubblica. A tal fine possono essere predisposti documenti programmatici, anche sulla base di indicazioni Interforze.

ART. 28 – Modalità da adottare per l'utilizzo degli impianti

1. L'utilizzo degli apparati da parte degli operatori e dei soggetti autorizzati al trattamento deve essere conforme alle finalità dell'impianto previste dal presente regolamento.

2. L'angolo di ripresa e la lunghezza focale delle telecamere devono essere impostati in modo tale da consentire il controllo e la registrazione di quanto accada in aree pubbliche o aperte al pubblico, con esclusione tassativa delle proprietà private, fatta salva specifica richiesta da parte dell'Autorità giudiziaria.

3. Fatti salvi i casi di richiesta da parte degli interessati, i dati relativi alle registrazioni possono essere esaminati, nel limite del tempo ammesso per la conservazione di cui all'articolo 31 del presente regolamento, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'articolo 25. Qualora dall'analisi siano rilevate informazioni rilevanti per i fini previsti, l'operatore autorizzato procede all'estrazione dell'immagine o della sequenza strettamente necessaria a documentare l'evento e alla memorizzazione su supporto fisso o mobile dedicato, protetto dalle necessarie misure di sicurezza volte a prevenire l'accesso o il trattamento non autorizzato o non conforme alla finalità della raccolta, dalla perdita, dalla distruzione o dal danno accidentali.

4. Ove, anche per gli impianti di videosorveglianza preposti ad altri scopi, dall'analisi delle immagini raccolte dovessero essere rilevate informazioni relative a fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica, ne verrà data immediata comunicazione agli organi competenti. Anche in tali casi si potrà procedere ad effettuare l'estrazione dei dati di ripresa strettamente necessari e non eccedenti ed alla memorizzazione su appositi supporti fissi o mobili, debitamente protetti. Le informazioni raccolte verranno comunicate solo agli organi di Polizia Giudiziaria e l'Autorità Giudiziaria. L'eventuale trasmissione del contenuto dovrà avvenire con modalità adeguatamente protette.

5. Qualsiasi apparato tramite il quale sono visibili le riprese, siano esse in diretta o in differita, dovranno essere disposti/collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee e non autorizzate.

6. Le informazioni ricavate dai dati rilevati possono essere utilizzati, in forma anonima, nel rispetto delle vigenti disposizioni di legge, a fini statistici e per studi, analisi e rilievi di traffico.

ART. 29 – Comunicazione e diffusione dei dati

1. La comunicazione dei dati acquisiti tramite i sistemi di videosorveglianza a favore dei soggetti pubblici richiedenti è ammessa solo quando è consentita da una norma di legge o di regolamento o da atti amministrativi generali per le finalità e con le modalità previste dall'articolo 2-ter del Decreto Legislativo 30 giugno 2003, n. 196.

2. Fatte salve le autonome acquisizioni di immagini nell'ambiti dei sistemi ad accesso condiviso regolati da specifici accordi, convenzioni e Patti territoriali con Enti del territorio e forze di polizia, è consentita la comunicazione di dati richiesti, in conformità alla normativa vigente, 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, per finalità di difesa o di sicurezza dello Stato, previa formale richiesta scritta.

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

4. Nell'ambito delle investigazioni difensive, il difensore della persona sottoposta alle indagini, a norma dell'art. 391-quater c.p.p., può richiedere ed acquisire copia delle riprese in formato digitale previo pagamento delle relative spese.

5. Il cittadino vittima o testimone di reato, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può richiedere che i filmati siano estratti e conservati oltre i termini previsti con le stesse modalità riservate all'esercizio dei diritti dell'interessato, 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.

6. È vietata ogni forma di diffusione delle immagini e dei dati raccolti tramite i sistemi di videosorveglianza, fatti salvi i casi in cui le riprese non consentano, neanche indirettamente facendo ricorso ad altre informazioni, l'individuazione e il riconoscimento di persone fisiche.

ART. 30 – Accesso agli impianti, ai dati e alla centrale di controllo

1. L'accesso agli impianti e alla Centrale di controllo è sottoposto a specifiche limitazioni e controlli ed è consentito solo al personale espressamente autorizzato, nonché al personale addetto alla manutenzione degli impianti e alla pulizia dei locali. L'elenco del personale autorizzato è manutenuto ed aggiornato dal Comandante della Polizia Municipale.

2. L'accesso agli impianti e la visualizzazione dei dati avviene di norma da postazioni dedicate collocate all'interno della Centrale Operativa della Polizia Municipale e delle Centrali Operative delle Forze dell'Ordine interconnesse con il sistema di videosorveglianza comunale nell'ambito degli accordi di cui all'articolo 25 del presente regolamento.

3. L'accesso ai dati dei sistemi è consentito ai soli soggetti autorizzati, muniti di credenziali di accesso valide e strettamente personali, che permettono un livello di operatività conforme al profilo di autorizzazione. La visualizzazione in diretta delle immagini e l'accesso ai dati conservati per la duplicazione e la loro differita visualizzazione è strutturata secondo distinti livelli di autorizzazione stabiliti con apposito atto dal del Comandante della Polizia Municipale., che conserva l'elenco aggiornato dei soggetti autorizzati. Ove consentito dal sistema in uso, gli accessi sono registrati e il registro è conservato per un periodo prestabilito. L'elenco dei soggetti autorizzati e il relativo profilo di autorizzazione comprende anche l'accesso a eventuali supporti di memorizzazione magneto-ottici, a memorie removibili e supporti di registrazione temporanea.

4. In caso di necessità, per operazioni di manutenzione e assistenza, le imprese affidatarie abilitate al servizio tecnico, mediante personale appositamente incaricato, possono accedere agli impianti, alla Centrale di controllo e ai sistemi di registrazione delle immagini registrate esclusivamente per le suddette necessità tecniche e nel rispetto degli obblighi di segretezza e riservatezza previste negli atti di cui all'articolo 8 del presente regolamento. L'accesso alle immagini registrate è consentito solo alla presenza di soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini registrate.

5. Eventuali accessi da parte di soggetti diversi da quelli previsti dai commi precedenti devono essere espressamente autorizzati dal Comandante della Polizia Municipale con specifica indicazione circa tempi, modalità e ragioni del medesimo ed avvengono alla presenza di soggetti autorizzati dotati delle specifiche credenziali

ART. 31 – Conservazione e custodia delle registrazione

1. Le registrazioni dei sistemi di videosorveglianza sono conservate con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati e cancellati o anonimizzati una volta decorso tale termine.

2. I tempi di conservazione dei dati personali raccolti e trattati con i sistemi di videosorveglianza di cui al presente regolamento, dipendono dalle normative riferimento sulla base della declinazione finalistica di ogni singolo impianto.

3. La conservazione di dati personali degli impianti preposti a finalità di sicurezza urbana ovvero repressione e prevenzione reati, di cui all'art. 25 del presente regolamento fa riferimento all'art. 3 comma 1 lett. e) del D.lgs. 51/2018, anche per ciò che concerne la durata della conservazione. Tale durata è definita anche in relazione a quanto previsto dai Patti Territoriali, dagli accordi con gli Enti del territorio, dal Comitato Provinciale per l'Ordine e la Sicurezza Pubblica o da accordi con Comitato provinciale. Decorso tale periodo, i dati registrati sono cancellati con modalità automatica.

4. La conservazione di dati personali degli impianti preposti alle restanti finalità previste dall'articolo 25 del presente regolamento sono conservati per un periodo di tempo pari a quanto previsto dalle normative di settore. Decorso tale periodo, i dati registrati sono cancellati, ove possibile con modalità automatiche.

5. Nei casi previsti dal comma 4 dell'articolo 25 del presente Regolamento, la conservazione separata dei dati estratti dai sistemi di registrazione a fini di elevare una sanzione amministrativa viene mantenuta sino alla conclusione del procedimento sanzionatorio a esso correlato.

6. Nei casi previsti dal comma 5 dell'articolo 25 del presente Regolamento, la conservazione separata dei dati estratti dai sistemi di registrazione, a fini amministrativi o di polizia giudiziaria, viene mantenuta sino alla trasmissione agli organi competenti o alla conclusione del processo investigativo, con il limite massimo di sei mesi.

7. La conservazione dei dati personali per un periodo di tempo superiore a quello indicato dai commi precedenti è ammessa esclusivamente su specifica richiesta della autorità giudiziaria o della polizia giudiziaria in relazione ad un'attività investigativa in corso.

8. Le registrazioni custodite presso i sistemi di videosorveglianza, le immagini e i filmati estratti per la conservazione ulteriore o per la comunicazione ad altri soggetti sono protette e custodite le misure di sicurezza definite all'articolo 15 del presente regolamento. Per i supporti che non prevedono sistemi di cancellazione automatica, i dati estratti devono essere cancellati manualmente immediatamente dopo la loro comunicazione o trasmissione o decorsi i tempi di conservazione previsti dal presente articolo.

ART. 32 –Sicurezza dei dati e dei sistemi

1. Nella progettazione, implementazione e sviluppo dei sistemi di videosorveglianza, l'Ente, anche tramite i soggetti affidatari della realizzazione tecnica degli impianti, mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio per gli interessati, misurato da una specifica analisi. Tali misure sono raccolte in un disciplinare tecnico interno, per quanto riguarda l'infrastruttura di proprietà del Comune e nei disciplinari tecnici dei fornitori dei servizi svolti mediante piattaforme in cloud volte ad assicurare:

a) la resilienza dei sistemi e la riservatezza, l'integrità e la disponibilità dei dati in essi contenuti o da questi veicolati;

b) il ripristino tempestivo della disponibilità e dell'accesso ai dati in caso di incidente;

c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento dei dati personali.

2. In presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto delle caratteristiche dei sistemi utilizzati, i soggetti autorizzati dovranno essere in possesso di specifiche credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascun, unicamente le operazioni di competenza.

3. Nei sistemi che ne permettono l'implementazione sono adottati meccanismi di cancellazione automatica delle registrazioni, allo scadere dei termini previsti, con le modalità previste dai disciplinari tecnici dei fornitori dei servizi e dal disciplinare interno .

4. Nei casi di trasmissione delle immagini attraverso reti pubbliche di comunicazione sono adottate misure tecnologiche adeguate, anche a mezzo di tecniche crittografiche, che garantiscano la sicurezza dei flussi di dati trasmessi con le modalità previste dai disciplinari tecnici dei fornitori dei servizi e da quello interno.

5. L'Ente adotta sistemi idonei alla registrazione degli accessi logici o fisici dei soggetti autorizzati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali con le modalità previste dai disciplinari tecnici dei fornitori dei servizi e dal manuale interno.

6. Come previsto dall'art. 35 del GDPR e dall'art. 23 del Decreto Legislativo 18 maggio 2018, n. 51, l'Ente redige e aggiorna le necessarie Valutazione d'impatto sulla protezione dei dati ed adotta le misure in esse previste, anche attraverso piani di adeguamento che verranno riportati nei disciplinari tecnici dei fornitori e dal manuale interno .

ART. 33 – Norme di rinvio

1. Per quanto non espressamente disciplinato dal presente regolamento, si rinvia a quanto disposto dalle norme di settore.