COMUNE DI CICONIO

Città Metropolitana di Torino

REGOLAMENTO D'ESERCIZIO DEL SISTEMA DI VIDEOSORVEGLIANZA DEL COMUNE DI CICONIO

Allegato alla D.C.C. N. 26 del 30.11.2018

IL SINDACO

IL SEGRETARIO COMUNALE

Indice

Art. 1 - Obiettivo del presente Regolamento

Obiettivo del presente regolamento è assicurare che i trattamenti di dati personali effettuati dal Comune di Ciconio nel territorio del Comune di Ciconio mediante il sistema di videosorveglianza, avvengano correttamente, lecitamente, e conformemente a quanto previsto dalla disciplina rilevante in materia di sicurezza e protezione dei dati personali; in particolare, il rispetto del presente regolamento garantirà la conformità:

- alle prescrizioni del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali);
- al Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003);
- ai provvedimenti del Garante per la protezione del dati personali, con particolare riferimento al provvedimento generale del 29 aprile 2004 del Garante per la protezione dei dati personali, dedicato alla videosorveglianza;
- ai principi di:
    - liceità;
    - necessità;
    - non eccedenza e proporzionalità;
    - finalità.

- Al Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito RGPD) 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”;
- Alla Direttiva UE 2016/680 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”;
- Al DPR n. 15 del 15/01/2018 recante “Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia”;
- Al Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell’8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- Al Decreto Ministero dell’Interno 05/08/2008 (GU n. 186 del 09.08.2008);
- Alla Legge n. 38/2009 recante “misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori”.

Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. La videosorveglianza dà luogo pertanto a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.

Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza gestiti ed impiegati dal Comune di CICONIO nel territorio comunale, 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. 2 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali, per brevità nel seguito chiamato anche semplicemente "*Codice*").

Ai sensi della vigente normativa si intende per:

a) "*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
b) "*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
c) "*dati identificativi*	i dati personali che permettono l'identificazione diretta dell'interessato;
d) "*dati sensibili*	i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
e) "dati giudiziari"	i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
f) "*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

g) "*responsabile*	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
h) "*incaricati*	la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del responsabile del trattamento
i) "*interessato*	la persona fisica cui si riferiscono i dati personali oggetto di trattamento
l) "*comunicazione*	il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
m) "*diffusione*	il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
n) "*dato anonimo*	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
o) "*blocco*	la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
p) "*banca di dati*	il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese
q) "*Garante*	L'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
r) "*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
s) "*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
t) "*misure minime*	il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
u) "*strumenti elettronici*	gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
v)"*autenticazione informatica*	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
z) "*credenziali di autenticazione*	i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

aa) "*parola chiave*	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
ab) "*profilo autorizzazione*	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica
ac) "*sistema autorizzazione*	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
ad) *"rischi*	Situazioni o comportamenti che possano generare un pericolo per i dati personali e/o sensibili. Per meglio valutare l'entità e le azioni da intraprendere il rischio prevede diversi livelli di soglia: basso, medio, grave o gravissimo;
ae) *"pseudonimizzazione*	il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

Art. 3 - Ambito di validità, di applicazione del presente regolamento

Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali effettuati mediante sistema di videosorveglianza:

- sotto la diretta titolarità del Comune di Ciconio
- all'interno del territorio del Comune di Ciconio.

Art. 4 - Identificazione del titolare del trattamento dei dati

Il titolare dei trattamenti di dati personali effettuati mediante il sistema di videosorveglianza del Comune di Ciconio è il Sindaco.

Pertanto competono esclusivamente al Comune di Ciconio le decisioni in ordine alle finalità e alle modalità del trattamento, compreso anche il profilo della sicurezza. A titolo esemplificativo e non esaustivo, si riportano di seguito alcune decisioni che spettano esclusivamente al Comune di Ciconio:

- il numero, la tipologia e i luoghi di installazione attuale e futura delle telecamere;
- i tempi massimi e minimi di memorizzazione delle immagini;

- gli strumenti elettronici, informatici e telematici da utilizzare per la gestione delle immagini, compresa la ripresa e la memorizzazione delle immagini stesse;
- l'individuazione dei soggetti che possono essere a vario titolo coinvolti (in qualità di incaricati, oppure di responsabili interni od esterni oppure di autonomi titolari) nelle operazioni di trattamento dai dati e nelle operazioni di amministrazione di gestione di sistema informatico e telematico;
- l'individuazione di compiti e responsabilità da assegnare ai soggetti individuati in precedenza.

Il Titolare del trattamento dei dati è il Comune di Ciconio, al quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

Il Responsabile dell'Area Tecnica è designato quale Responsabile del trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza.

Il Responsabile del trattamento è tenuto a conformare la propria azione al pieno rispetto di quanto prescritto dalle vigenti disposizioni normative in materia e dal presente Regolamento.

Il Responsabile procede al trattamento dei dati attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

Le competenze proprie del Responsabile del trattamento sono analiticamente disciplinate nel contratto ovvero nell'atto giuridico avente forma scritta, con il quale il Titolare provvede alla sua designazione. In particolare:

- il Responsabile del trattamento individuerà e nominerà con propri atti gli Incaricati del trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, RGPD; detti incaricati saranno opportunamente istruiti e formati da parte del Responsabile del trattamento con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;
- il Responsabile del trattamento provvede a rendere l'informativa "minima" agli interessati secondo quanto definito al precedente art. 6;
- il Responsabile del trattamento verifica e controlla che il trattamento dei dati effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui all'art. 5 del RGPD e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;
- il Responsabile del trattamento assicura che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

- il Responsabile del trattamento, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;

- il Responsabile del trattamento assiste il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;

- il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32, RGPD, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;

- il Responsabile del trattamento garantisce l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente;

- il Responsabile del trattamento assicura l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;

- il Responsabile del trattamento assiste il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;

- il Responsabile del trattamento assiste il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e del precedente art. 7 del presente Regolamento e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;

- il Responsabile del trattamento affianca il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;

- il Responsabile del trattamento garantisce che il Responsabile della Protezione dei Dati designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;

- il Responsabile del trattamento mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;

- il Responsabile del trattamento è responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

- il Responsabile del trattamento assicura che gli incaricati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;

- il Responsabile del trattamento garantisce la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale individuato quale incaricato con riferimento ai trattamenti realizzati mediante l'impianto di videosorveglianza dell'Ente, previo consulto del Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;

- il Responsabile del trattamento vigila sul rispetto da parte degli incaricati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Il Responsabile interno del trattamento è autorizzato a ricorrere a Responsabili esterni del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato, in tutti i casi in cui egli, per la gestione/assistenza del sistema di videosorveglianza, faccia ricorso a soggetti esterni ai quali affidare incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Ente. In questi casi, il Responsabile interno del trattamento procederà a disciplinare i trattamenti da parte del responsabile esterno mediante contratto ovvero altro atto giuridico che vincoli il Responsabile esterno del trattamento al Titolare del trattamento ai sensi dell'art. 28, RGPD

Art. 5 - Obiettivi e finalità del sistema di videosorveglianza

Il sistema di videosorveglianza, in quanto sistema che comporta il trattamento di dati personali, può venire utilizzato (ai sensi dell'art. 18 comma 2 del D.Lgs. 196/2003) esclusivamente per il perseguimento delle funzioni istituzionali del titolare del trattamento dei dati, vale a dire del Comune di Ciconio.

Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza attengono allo svolgimento delle funzioni istituzionali proprie dell'amministrazione comunale in conformità a quanto previsto dal:

- D. Lgs. 18 agosto 2000, n. 267 – TUEL;

- D.P.R. 24 luglio 1977, n.616;

- D. Lgs. 31 marzo 1998, n. 112;

- Legge 7 marzo 1986, n. 65, sull'ordinamento della Polizia Municipale;

- Legge 24 luglio 2008, n. 125 recante misure urgenti in materia di sicurezza pubblica;

- Legge 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale;
- Decreto del Ministero dell'Interno del 5 agosto 2008 in materia di incolumità pubblica e sicurezza urbana;
- Circolari del Ministero dell'Interno n.558/A/421.2/70/456 in data 8 febbraio 2005, n. 558/A421.2/70/195860 in data 6 agosto 2010 e n. 558/SICPART/421.2/70/224632 in data 2.3.2012.

Nella richiamata cornice normativa e all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica, l'impianto di videosorveglianza del Comune di Ciconio, è precipuamente rivolto a garantire la sicurezza urbana che, l'art. 1 del Decreto del Ministero dell'Interno del 5 agosto del 2008, testualmente definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."

La disponibilità tempestiva di immagini presso il Comune costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione della Polizia Locale sul territorio comunale, in stretto raccordo con le altre forze dell'ordine. L'archivio dei dati registrati costituisce, infatti, per il tempo di conservazione stabilito per legge, un patrimonio informativo per finalità di Polizia Giudiziaria, con eventuale informativa nei confronti dell'Autorità Giudiziaria competente a procedere in caso di rilevata commissione di reati.

In particolare, il sistema di videosorveglianza attivato dall'Amministrazione, è finalizzato a:

a) incrementare la sicurezza urbana e la sicurezza pubblica nonché la percezione delle stesse rilevando situazioni di pericolo e consentendo l'intervento degli operatori;

b) prevenire, accertare e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" già richiamato; le informazioni potranno essere condivise con altre forze di Polizia competenti a procedere nei casi di commissione di reati;

c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;

d) controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico;

e) al monitoraggio del traffico;

f) attivare uno strumento operativo di protezione civile sul territorio comunale;

g) ad acquisire elementi probatori in fattispecie di violazioni amministrative o penali;

h) per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;

i) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;

j) verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti.

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. Gli impianti di videosorveglianza non potranno altresì essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.

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.

La possibilità di avere in tempo reale dati e 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, 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.

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.

Art. 6 - Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità, e finalità.

6.1 Premessa

La verifica del rispetto dei principi di liceità, necessità, non eccedenza e proporzionalità e finalità dovrà venire effettuata periodicamente sia nei confronti del sistema di videosorveglianza nel suo complesso, sia nei confronti di ciascuna telecamera installata.

6.2 Principio di liceità

Il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6, Paragrafo 1, lett. e), RGPD. La videosorveglianza comunale pertanto è consentita senza necessità di consenso da parte degli interessati.

Affinché sia soddisfatto il principio di liceità, si dovrà verificare e assicurare che:

- le finalità perseguite mediante il sistema di videosorveglianza siano coerenti e compatibili con le funzioni istituzionali di competenza del Comune di Ciconio;

- la videosorveglianza non avvenga in violazione delle vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata (es. art. 615bis del Codice Penale), di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela;
- la videosorveglianza non abbia luogo in violazione delle tutele riconosciute ai lavoratori, con particolare riferimento a quanto previsto dalla Legge 300/1970 (Statuto dei Lavoratori);
- le riprese o le registrazioni non vengano effettuate in violazione di quanto previsto da disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi;
- la videosorveglianza avvenga nel rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni;
- siano osservati specifici limiti derivanti da disposizioni di legge o di regolamento che prevedono o ipotizzano la possibilità di installare apparecchiature di ripresa locale, aerea o satellitare (d.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, dalla legge 24 aprile 2003, n. 88), disposizioni che, quando sono trattati dati relativi a persone identificate o identificabili, vanno applicate nel rispetto dei principi affermati dal Codice, in tema per esempio di sicurezza presso stadi e impianti sportivi.

6.3 Principio di necessità

In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.

Affinché sia rispettato il principio di necessità deve essere escluso qualsiasi utilizzo superfluo ed evitati eccessi e ridondanze. Inoltre il sistema informatico e ciascuna telecamera deve essere configurata ed utilizzata in maniera tale da non utilizzare dati relativi a soggetti identificabili quando le finalità del trattamento possono essere perseguite raccogliendo solamente dati anonimi; inoltre il software deve essere configurato in modo da cancellare automaticamente e periodicamente i dati eventualmente registrati.

Ulteriori considerazioni da tenere presenti per il rispetto del principio di necessità sono le seguenti:

- l'esigenza di perseguire le finalità deve essere concreta, reale e comprovabile;
- il personale dipendente comunale, non potendo avere una diffusione e una presenza capillare sul territorio, non è in grado di assicurare il monitoraggio e la registrazione continua dei fatti, che solo un sistema di videosorveglianza può assicurare;

- da un punto di vista economico, l'utilizzo di un sistema elettronico di videosorveglianza presenta dei costi sensibilmente inferiori rispetto ai costi derivanti dall'utilizzo di personale dedicato al perseguimento delle finalità indicate in precedenza;

- il sistema di videosorveglianza deve essere configurato 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.

6.4 Principio di non eccedenza e proporzionalità

La raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente 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 quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.

Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere.

Il rispetto dei principi di non eccedenza e proporzionalità si dovrà valutare periodicamente con riferimento ai criteri di seguito elencati:

- il numero e la collocazione delle telecamere devono essere effettivamente commisurate al reale livello di rischio, evitando la rilevazione o la registrazione in aree che non siano soggette a concreti pericoli o che non siano meritevoli di particolare tutela;

- il posizionamento, la tipologia di telecamere, le aree brandeggiabili, l'utilizzo di zoom, quali dati ed eventi rilevare, devono essere rapportati alle concrete finalità ed esigenze, e si dovranno evitare eccedenze; ad esempio si dovrà limitare la possibilità di brandeggio mediante l'impostazione di vincoli o di mascheramenti statici;

- le telecamere devono essere collocate, e più in generale la videosorveglianza deve essere adottata, solo quando altre misure meno "invasive" siano state ponderatamente valutate insufficienti o inattuabili;

- se l'installazione delle telecamere è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri accorgimenti quali ad esempio controlli da parte di addetti, sistemi di allarme, misure di protezione perimetrale e degli ingressi, abilitazione e controllo degli accessi;

- non è consentita l'installazione meramente dimostrativa o artefatta di telecamere non funzionanti o per finzione, che può essere legittimamente oggetto di contestazione;
- la non eccedenza e proporzionalità deve essere valutata, anche periodicamente, in ogni fase e modalità del trattamento; ad esempio, in fase di definizione e assegnazione dei profili di accesso ai dati, i profili dovranno essere configurati e assegnati in maniera che gli incaricati accedano alla minima quantità di dati necessaria per lo svolgimento dei compiti assegnati; come minimo si dovrà prevedere una fondamentale distinzione tra il profilo di tipo "utente normale" e un profilo più elevato di tipo "*administrator*";

6.5 Principio di finalità

Ai sensi dell'art. 5, Paragrafo 1, lett. b), RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana che il DM Interno 05/08/2008 definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."

Gli scopi perseguiti devono essere determinati, espliciti e legittimi, ai sensi dell'art. 11 comma 1 lett. b) del D.Lgs. 196/2003; sono pertanto esclusi utilizzi indeterminati, occulti e non legittimi. In particolare il titolare o il responsabile potranno perseguire solo finalità di sua pertinenza.

Potranno essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria). E non finalità generiche o indeterminate, soprattutto quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti.

E' inoltre consentita la videosorveglianza come misura complementare volta a supportare 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 o riprese, in caso di atti illeciti.

Art. 7 - Utilizzi esplicitamente vietati di sistemi di sorveglianza

Nell'intero territorio del Comune di Ciconio è fatto divieto di posizionare telecamere, ed in ogni caso di utilizzare immagini e/o registrazioni provenienti da sistemi di videosorveglianza orientati verso luoghi aperti e di pubblico passaggio e/o utilizzo, ai privati cittadini. Si intendono fatte salve le installazioni di videocitofoni.

In luoghi chiusi, siano essi pubblici o privati, vige tale divieto. Nel caso si presenti l'esigenza chiaramente dimostrabile e giustificabile, di effettuare riprese in luoghi chiusi pubblici o aperti al pubblico, si dovrà verificare e assicurare che le riprese avvengano nel pieno rispetto dello "Statuto dei lavoratori" e non violino il divieto, da parte del datore di lavoro, di effettuare controlli a distanza sull'attività dei dipendenti. In tali luoghi dovrà essere esposta una cartellonistica informativa riportante l'indicazione "LOCALE SOTTOPOSTO A VIDEOSORVEGLIANZA INTERNA PER MOTIVI DI SICUREZZA"

E fatto divieto di posizionare telecamere e più in generale di utilizzare il sistema di videosorveglianza al solo fine di controllare il rispetto del divieto di fumare o gettare mozziconi, di calpestare aiuole, di affiggere o di fotografare, o di altri divieti relativi alle modalità nel depositare i sacchetti di immondizia entro gli appositi contenitori.

Relativamente al controllo e alla tutela di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose, il sistema di videosorveglianza potrà venire utilizzato solo se saranno in maniera chiara e documentata risultate inefficaci o inattuabili altre misure. Il medesimo controllo non è invece lecito, e va effettuato sotto altra forma, se è volto ad accertare solo infrazioni amministrative rispetto a disposizioni concernenti modalità e orario di deposito dei rifiuti urbani.

Art. 8 - Utilizzi particolari

Qualora il sistema di videosorveglianza venga utilizzato a fini di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, si dovrà rispettare quanto dettato dal d.P.R. 22 giugno 1999, n. 250. Tale normativa impone al titolare del trattamento dei dati, quindi al Comune di Ciconio, di richiedere una specifica autorizzazione amministrativa, nonché di limitare la raccolta dei dati sugli accessi rilevando le immagini solo in caso di infrazione (art. 3 d.P.R. n. 250/1999). In questo specifico caso e utilizzo, i dati trattati potranno essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso e si potrà accedere ad essi solo a fini di polizia giudiziaria o di indagine penale.

Art. 9 - Tipi di trattamenti autorizzati e modalità di trattamento

Nell'installazione e nell'esercizio del sistema di videosorveglianza, sono autorizzati esclusivamente le seguenti tipologie di trattamenti:

- installazione e attivazione di nuove telecamere;
- creazione e gestione di gruppi e profili di utenti;
- consultazione immagini live da telecamera;
- messa a fuoco e brandeggiamento della telecamera;
- impostazione di limiti al brandeggiamento delle telecamere
- impostazione di zone oscurate staticamente
- registrazione di immagini;
- cancellazione di immagini;
- predisposizione delle soglie temporali e degli eventi di cancellazione immagini;
- consultazione immagini registrate;
- estrazione (duplicazione) immagini registrate;
- definizione aree di motion-detection;
- definizione azioni da eseguire in concomitanza di eventi di motion-detection;

- accensione di sorgenti luminose o ad infrarosso;
- attivazione funzionalità di “speak-ip”;
- rilevazione e inventario degli indirizzi ip presenti in rete;
- rilevazione e inventario dei mac address presenti in rete;
- installazione e configurazione di software applicativo;
- installazione e configurazione di software di base;
- installazione di “patch” e “hot fix”;
- attivazione collegamenti da remoto;
- interventi generici di manutenzione e configurazione hardware e software.

L’installazione delle telecamere avviene esclusivamente nei luoghi pubblici (strade, piazze, immobili) in conformità all’elenco dei siti di ripresa predisposto dall’Amministrazione Comunale.

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.

Le telecamere di cui al precedente comma 1, consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario.

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. I segnali video delle unità di ripresa saranno inviati presso l’Unita di ricezione, registrazione e visione ubicata nell’Ufficio Polizia Municipale. In questa sede le immagini saranno visualizzate su monitor e registrate su supporto magnetico.

I dati personali oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;

- raccolti e registrati per le finalità di cui all’art. 4 del presente Regolamento e resi utilizzabili in altre operazioni di trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;

- raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l’uso di sistemi di videosorveglianza è limitata al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell’autorità giudiziaria o di polizia giudiziaria.

Nelle sole ipotesi in cui l’attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle richiamate disposizioni normative, il termine massimo di durata della conservazione dei dati è

limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve specifiche esigenze di ulteriore conservazione.

In ragione di necessità investigative e su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria il Responsabile potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai sette giorni previa richiesta al Garante per la protezione dei dati personali che, a seguito di verifica preliminare, potrà rilasciare parere favorevole.

Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato l´integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Art. 10 - Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati

Le operazioni di trattamento dei dati saranno svolte – a vario titolo – dalle seguenti tipologie di soggetti:

- Titolare del trattamento dei dati;
- Responsabile del trattamento dei dati; il Responsabile del trattamento dei dati (relativamente al sistema di Videosorveglianza) è individuato nella persona del Responsabile del Servizio dell'attività di videosorveglianza, nominato dal Sindaco con atto scritto; l'atto di nomina dovrà specificare dettagliatamente le istruzioni e i compiti affidati al Responsabile del trattamento dei dati;
- Responsabile esterno del trattamento dei dati: sono i soggetti (persone fisiche o giuridiche) esterni al Comune di Ciconio ai quali sono affidati, da parte del Comune di Ciconio, alcune operazioni di trattamento dei dati e la messa in atto di alcune misure di sicurezza;
- Incaricati del trattamento dei dati: sono i soggetti fisici (persone fisiche) che, designati per iscritto dal titolare o dal responsabile, eseguono una o più operazioni di trattamento dei dati; il profilo e l'ambito del trattamento consentito agli incaricati dovrà essere tale da permettere a questi la sola consultazione delle immagini in diretta e delle immagini registrate;
- Custode delle password di sistema: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell'amministratore di sistema - delle parole chiave corrispondenti ai vari profili di tipo "administrator" o equivalenti;
- Custode delle parole chiave: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell'incaricato delle parole chiave assegnate agli utenti finali;
- Soggetti incaricati della gestione e manutenzione degli strumenti elettronici, denominati anche "Amministratori di sistema";
- Altre Pubbliche Amministrazioni che richiedano di accedere ai dati per lo svolgimento delle loro funzioni istituzionali: in questo caso l'accesso e l'utilizzo dei dati messi a disposizione dal Comune di Ciconio, avrà luogo sotto la diretta responsabilità e titolarità della Pubblica Amministrazione o del soggetto richiedente: sarà pertanto cura della Pubblica Amministrazione o

del soggetto richiedente verificare che l'accesso avvenga esclusivamente per lo svolgimento delle funzioni istituzionali, e non per il perseguimento di interessi o finalità personali o comunque non chiaramente riconducibili allo svolgimento di funzioni istituzionali o di compiti d'ufficio, senza che vi sia abuso d'ufficio. Sarà inoltre cura della Pubblica Amministrazione o del soggetto richiedente, o del soggetto al quale i dati sono comunicati o portati a conoscenza a seguito di motivata richiesta, mettere in atto quanto previsto dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento all'obbligo di designazione degli incaricati del trattamento, specificando puntualmente per iscritto l'ambito del trattamento consentito e assicurando che le operazioni di trattamento (compresa la mera consultazione, che è comunque una tipologia di trattamento) e l'accesso ai dati avvenga in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Art. 11 - Accesso ai dati da parte delle forze dell'ordine e dell'Autorità Giudiziaria

Il D.Lgs. 196/2003 prevede (art. 19) che la comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico possa avvenire se:

- prevista da norma di legge o di regolamento, oppure
- anche in assenza di norma di legge o di regolamento, sia necessaria per lo svolgimento delle funzioni istituzionali.

Pertanto le Forze dell'Ordine o l'Autorità Giudiziaria possono lecitamente richiedere di:

- accedere alle immagine live"
- accedere alle immagini registrate ed ottenete copia delle registrazioni
- effettuare riprese e registrazioni ad-hoc".

La mancata o tardiva concessione dell'accesso potrà comportare, a carico del soggetto responsabile, il reato di omissione di atti d'ufficio e di ostacolo alle indagini.

Le richieste di accesso/estrazioni dovranno seguire le procedure definite nel presente regolamento, ed essere autorizzate dal Sindaco o dal Responsabile del trattamento dei dati relativamente alla videosorveglianza.

In ogni caso, l'utilizzo delle immagini da parte di qualsiasi soggetto pubblico che per l'esercizio delle proprie funzioni istituzionali abbia necessità di accedere ai dati, dovrà avvenire conformemente a quanto previsto dal D.Lgs. 196/2003 e più in generale dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento al provvedimento generale del Garante per la protezione dei dati personali del 29 aprile 2004, dedicato alla videosorveglianza.

Il Comune di Ciconio provvederà a fornire, al competente Comando dei Carabinieri di Agliè, le necessarie credenziali di accesso all'applicativo di controllo remoto del Sistema di rilevazione e gestione installato.

L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 del presente Regolamento.

L'accesso alle immagini è consentito esclusivamente:

a) al Titolare, al Responsabile ed agli incaricati dello 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, secondo la procedura descritta al successivo art. 13. 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 responsabile 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;

e) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

Art. 12 - Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento

Il Responsabile del trattamento dei dati procede ad individuare con proprio atto, le persone fisiche incaricate del trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni.

L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun incaricato.

In ogni caso, prima dell'utilizzo degli impianti, gli incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.

Gli Incaricati procedono al trattamento attenendosi alle istruzioni impartite dal Responsabile il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

In particolare, gli incaricati devono:

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

- conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
- custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile del trattamento dei dati;
- mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
- conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
- fornire al Responsabile del trattamento dei dati ed al Responsabile della Protezione dei dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Tra i soggetti designati quali incaricati verranno individuati, con l'atto di nomina, le persone cui è affidata la custodia e la conservazione delle chiavi di accesso alla sala operativa ed agli armadi per la conservazione dei supporti magnetici.

Gli Incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alla istruzione del Titolare o del Responsabile.

L'utilizzo degli apparecchi di ripresa da parte degli Incaricati al trattamento dovrà essere conforme ai limiti indicati dal presente Regolamento come eventualmente modificato ed integrato.

Art. 13 - Obblighi degli incaricati/operatori

L'utilizzo delle telecamere è consentito solo per la sorveglianza di quanto è ubicato oppure si svolge nelle aree pubbliche o di proprietà comunale. Fatti salvi i casi di richiesta degli interessati, i dati registrati possono essere riesaminati, nel limite di tempo ammesso dal presente regolamento, solo in caso di effettiva necessità e per l'esclusivo perseguimento delle finalità di cui all'art. 5. In ogni caso, l'estrazione di immagini potrà avvenire solo in caso di richiesta/autorizzazione scritta da parte del Sindaco o del Comandante la Polizia Locale, oppure di richiesta proveniente da altra Pubblica Amministrazione, nei casi in cui l'accesso a immagini registrate sia necessario per lo svolgimento delle funzioni istituzionali. Anche in questo ultimo caso l'accesso/estrazione delle immagini dovrà essere autorizzata dal Sindaco oppure dal Responsabile del trattamento dei dati.

La mancata osservanza degli obblighi di cui al presente articolo potrà comportare l'applicazione di sanzioni disciplinari ed amministrative, e, ove previsto dalla vigente normativa, l'avvio di procedimenti penali.

Art. 14 - Tempi di conservazione delle immagini

In considerazione delle finalità individuate in precedenza, e della necessità di ottemperare al principio di non eccedenza e proporzionalità in tutte le operazioni di trattamento dei dati, le immagini registrate dovranno essere conservate per un tempo massimo di 7 giorni successivi alla rilevazione fatte salve speciali esigenze di ulteriore conservazione. Dovrà comunque essere presente una funzionalità che permetta agevolmente di disattivare la cancellazione automatica trascorso il tempo massimo di registrazione - delle immagini registrate (ad esempio in concomitanza della registrazione di atti vandalici), senza impedire o menomare la capacità di registrare le immagini in diretta. E inoltre prevista la possibilità che i tempi di memorizzazione delle immagini possano venire modificati a seguito di variazioni nelle finalità, di mutate esigenze, oppure di motivata richiesta proveniente da altri soggetti pubblici.

Art. 15 - Luogo e modalità di memorizzazione delle immagini

La immagini riprese dalle telecamere dovranno venire memorizzate in formato elettronico su un unico (o un numero limitato) supporto di memorizzazione di massa centralizzato e ben individuato all'interno di un unico e ben determinato apparato di tipo "server" (può essere comunque fatta salva la necessità di una memorizzazione di backup"su di un server remoto). Il suddetto server dovrà essere dedicato esclusivamente alla memorizzazione delle immagini registrate dalle telecamere del sistema di videosorveglianza, e non dovrà essere dedicato ad altri scopi. Se non diversamente disposto dal titolare con atto scritto, il server non dovrà essere collegato ad internet, oppure dovrà essere collegato solo in casi e per finalità specifiche e ben individuate, per intervalli di tempo il più possibile contenuti.

Non è consentita la memorizzazione "ordinaria" delle immagini in locale a livello di postazione "client", o comunque su supporti e strumenti diversi dal succitato server centralizzato. La memorizzazione temporanea delle immagini in locale potrà avvenire solo in caso di estrazione di immagini, nel qual caso la copia temporanea locale delle immagini estratte dovrà essere cancellata non appena possibile.

Presso il Comune è posizionato il monitor per la visione in diretta delle immagini riprese dalle telecamere e le apparecchiature per la relativa registrazione.

Il sistema è installato al piano Terreno dell'edificio comunale in stanza chiusa a chiave adibita allo scopo, all'interno di un mobile rack anch'esso chiuso a chiave.

Il sistema di registrazione NVR su server Rack, registra in Hdd e i dati sono visualizzabili attraverso un monitor al quale il sistema NVR è collegato.

Il sistema è protetto da un Ups che garantisce il funzionamento anche in mancanza di alimentazione diretta per un congruo periodo.

I dati sono accessibili dal responsabile di polizia locale che ha le chiavi di accesso del sistema, sia fisiche che software.

I dati sono estrapolabili Via USB con pen drive o con Hdd portatile;

Le telecamere IP sono marca HIKVISION

Il software di registrazione e gestione è un software proprietario e si chiama HIKVISION.

Le telecamere IP sono in tutto 15 di cui 3 collegate direttamente via cavo di rete e le altre con ponti radio (TP-LINK ACC. POINT 5GHZ 300MBPS OUTDOOR WIRELESS CPE510) che trasmettono direttamente in comune, attraverso un'infrastruttura studiata per mappare il più possibile l'abitato.

La scelta e la posizione delle telecamere è stata fatta di concerto fra l'Amministrazione Comunale e le principali Forze dell'Ordine, prioritariamente all'esigenza di monitorare il traffico da e per il centro abitato, ma anche le scuole, i parchi e le principali strutture pubbliche.

Il collegamento all'impianto di videosorveglianza può essere esteso alle Forze di Polizia che ne facciano richiesta all'amministrazione comunale, nei limiti e con l'osservanza delle norme contenute nel presente Regolamento ovvero disciplinate con successivo atto in conformità al quadro normativo di riferimento.

In relazione ai principi di pertinenza e di non eccedenza già richiamati all'art. 2 del presente Regolamento, il sistema informativo ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 16 - Criteri e modalità di estrazione delle immagini

L'estrazione di immagini o di intere riprese, mediante duplicazione e senza che vi sia cancellazione delle immagini registrate, potrà avvenire solo in presenza di autorizzazione scritta da parte del Sindaco del Comune di Ciconio o del Responsabile del trattamento dei dati, rilasciata a fronte di richiesta scritta e motivata.

La richiesta di estrazione dovrà specificare chiaramente il luogo o la telecamera di registrazione, e un'indicazione dell'intervallo temporale da estrarre e collocare su supporto esterno di memorizzazione di massa, come ad esempio cd-rom o DVD. In generale, le operazioni di estrazione dovranno essere effettuate dall'operatore (appositamente incaricato) in maniera tale che non vi sia accesso o conoscenza, da parte dell'operatore stesso, al contenuto delle immagini da estrarre.

All'atto della consegna al soggetto richiedente del supporto di memorizzazione contenente le immagini estratte, l'operatore o comunque chi materialmente consegnerà il suddetto supporto di memorizzazione, dovrà far firmare e trattenere apposito documento che attesti la consegna e la ricevuta delle immagini estratte; detto documento dovrà fare riferimento alla richiesta originaria di estrazione. Si dovrà inoltre aver cura di trattenere copia (su un secondo cd-rom o DVD) e custodire in cassaforte o in armadio metallico dotato di serratura e chiave funzionante, delle immagini estratte e consegnate. Il cd-rom contenente la copia delle immagini estratte dovrà essere protocollato, recare sul lato esterno con pennarello indelebile la data e l'ora di estrazione, il numero di protocollo, e la firma del soggetto che ha materialmente masterizzato il cd-rom.

Detto cd-rom dovrà immediatamente essere collocato in busta chiusa sigillata, recante sul lato esterno i seguenti dati:

- Numero di protocollo del cd-rom

- Data e ora di creazione del cd-rom
- Soggetto che ha richiesto l'estrazione
- Numero di protocollo della richiesta di estrazione
- Nome, cognome e firma del soggetto che ha materialmente masterizzato il cd-rom.

Si dovrà inoltre compilare apposito registro dove si terrà traccia di:

- Soggetto che ha richiesto l'estrazione
- Generalità del soggetto che ha materialmente ritirato con mani proprie il cd-rom
- Motivazione della richiesta di estrazione
- Numero di protocollo della richiesta di estrazione
- Numero di protocollo o riferimento univoco dell'autorizzazione all'estrazione
- Generalità del soggetto che ha materialmente effettuato la masterizzazione del cd-rom
- Giorno, data e ora di effettuazione dell'estrazione
- Numero di protocollo o identificazione univoca della ricevuta
- Numero di protocollo del cd-rom contenente la copia delle immagini estratte e consegnate al soggetto richiedente.

Per le richieste di estrazione di immagini provenienti da cittadini o più in generale da interessati, esercitate ai sensi dell'art. 7 del D.Lgs. 196/2003, potrà essere richiesto un contributo alle spese di ricerca ed estrazione delle immagini, ai sensi dell'art. 10 commi 7, 8 e 9 del D.Lgs. 196/2003, in ogni caso non eccedente la somma di Euro 50,00.

Art. 17 - Installazione di nuove telecamere

L'installazione di nuove telecamere dovrà essere autorizzata mediante atto deliberativo di Giunta Comunale. Preventivamente si dovrà verificare che:

- i luoghi ripresi;
- le telecamere utilizzate;
- le configurazione e la possibilità di utilizzo delle telecamere delle riprese e delle registrazioni effettuate;

soddisfino i principi di liceità, necessità, non eccedenza e proporzionalità e finalità.

Si dovrà inoltre tenere conto della dislocazione e delle finalità delle telecamere già installate; in ogni caso si dovrà aggiornare l'inventario dei luoghi e delle telecamere installate, che trovasi depositato agli Atti del responsabile del servizio di videosorveglianza.

Art. 18 - Informativa

I cittadini devono essere informati che si trovano o che stanno per accedere in una zona videosorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa minima, che dovrà riportare la dicitura :

Comune di Ciconio
Comune sottoposto a Videosorveglianza
Responsabile trattamento dati Comune di Ciconio

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive). A tal fine l'Ente utilizzerà lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, riportato in fac-simile nell´allegato n. 1 al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010 e di seguito richiamato:

L'Ente, in particolare, si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere, su cui è riportata la seguente dicitura: "Area videosorvegliata – la registrazione è effettuata dal Comune di CICONIO, per fini di sicurezza urbana, incolumità e ordine pubblico".

La segnaletica deve essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.

In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.

L'Ente, nella persona del Responsabile del trattamento dei dati, si obbliga ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

Art. 19 – Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, su presentazione di apposita istanza, ha diritto:

a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;

b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;

c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.

L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sulla home page del sito istituzionale dell'Ente alla Sezione "Privacy") ovvero al Responsabile del trattamento dei dati individuato nel Responsabile dell'Area Tecnica.

Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:

- il luogo, la data e la fascia oraria della possibile ripresa;
- l'abbigliamento indossato al momento della possibile ripresa;
- gli eventuali accessori in uso al momento della possibile ripresa;
- l'eventuale presenza di accompagnatori al momento della possibile ripresa;
- l'eventuale attività svolta al momento della possibile ripresa;
- eventuali ulteriori elementi utili all'identificazione dell'interessato.

Il responsabile della protezione dei dati dell'Ente ovvero il responsabile del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento

positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.

Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.

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.

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. L'interessato può altresì farsi assistere da persona di fiducia.

Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

In caso di esercizio da parte degli interessati dei diritti previsti dall'art. 7 del D.Lgs. 196/2003, il riscontro all'interessato dovrà venire fornito a cura del Titolare o da Responsabile del trattamento dei dati appositamente designato dal Titolare, **entro 30 giorni lavorativi dalla data di ricezione della richiesta**. Le richieste di cancellazione o blocco dei dati dovranno essere soddisfatte esclusivamente nei casi in cui il trattamento sia avvenuto in violazione di legge, e comunque solo su autorizzazione scritta del Sindaco di

Ciconio. Non potranno essere oggetto di cancellazione o modifica le immagini per le quali vi siano state richieste di estrazione o siano in corso indagini da parte degli organi di Polizia o da parte dell'Autorità Giudiziaria.

Art. 20 - Requisiti minimi sul luogo di collocazione del server

Il server di memorizzazione delle immagini è fisicamente collocato all'interno di un locale che fornisce adeguate garanzie di sicurezza fisica e perimetrale. Di seguito si riportano i requisiti minimi che il locale dovrà soddisfare:

- locale ad utilizzo esclusivamente a sala macchine, o sala server, non agevolmente accessibile al pubblico e ai dipendenti (ad eccezione ovviamente dei dipendenti o collaboratori esplicitamente incaricati di operazioni di amministrazione e gestione di sistema);
- possibilità di regolamentare e di tenere traccia degli accessi al locale;
- locale di norma chiuso a chiave, con serratura e chiave funzionante;
- in caso vi siano finestre a piano terra, presenza di inferriate in ferro non dolce oppure presenza di vetri antisfondamento;
- assenza di carta, cartoni o altro materiale facilmente infiammabile all'interno del locale;
- presenza nelle vicinanze di almeno un estintore non a polvere, funzionante e regolarmente revisionato con frequenza almeno semestrale;
- presenza di adeguato impianto di condizionamento, che assicuri un livello di umidità e temperatura all'interno del range di corretto funzionamento degli apparati;
- presenza di adeguati gruppi di continuità che possano assicurare la continuità dell'alimentazione elettrica in caso di interruzioni o di blackout.

In aggiunta a quanto elencato, è auspicabile (ancorché non strettamente obbligatoria) la presenza di quanto segue:

- allarme volumetrico (attivato dalla variazione della volumetria all'interno dei locali) o di prossimità;
- presenza di sensori per la rilevazione del fumo e/o della temperatura;
- collegamento dei sensori e dell'allarme con centrale operativa di sicurezza oppure con le forze dell'ordine.

Art. 21 - Iniziale deroga ai requisiti minimi sul luogo di collocazione del server

E' comunque previsto dal presente regolamento che, a causa di vincoli e problematiche di varia natura, sia possibile collocare il server in un luogo che non soddisfi, soprattutto in una fase iniziale, tutti i requisiti elencati nel precedente articolo. In tal caso sarà sufficiente verificare e assicurare che il server, e più in

generale gli apparati coinvolti, non siano a rischio palese di asportazione, danneggiamento o manomissione. Ad esempio, potrà essere giudicata come temporaneamente accettabile una situazione in cui il server non sia collocato in un locale ad utilizzo dedicato, ma sia collocato un ufficio dove il personale presente negli orari d'ufficio possa assicurare a vista un adeguato presidio e controllo. Negli orari di chiusura ufficio o in caso di assenza di personale, potrà essere ritenuta sufficiente la presenza di una porta che sia però dotata di serratura e chiave funzionante, e possa essere tenuta chiusa in caso di assenza di personale.

Art. 22 - Requisiti minimi sugli strumenti elettronici, informatici e telematici.

Gli strumenti elettronici, informatici e telematici utilizzati nelle operazioni di trattamento dei dati, dovranno soddisfare i seguenti requisiti minimi:

- sistema operativo server e client non obsoleto e con supporto attivo da parte del fornitore; non sono consentiti sistemi operativi obsoleti o poco sicuri come ad esempio Windows 95 oppure Windows 98;
- server e client protetti da password iniziale di accesso al sistema operativo e alle risorse di rete; possibilità da parte dell'utente finale di modificare autonomamente la propria password; possibilità da parte dell'amministratore di sistema di disabilitare la user-id senza cancellarla;
- server e client protetti da password iniziale di accesso al programma applicativo; possibilità da parte dell'utente finale di modificare autonomamente le propria password; possibilità di disabilitare (da parte dell'amministratore di sistema) le user-id senza cancellarla;
- presenza di almeno due profili distinti: uno di tipo "administrator" e uno di tipo "utente normale", sia a livello di sistema operativo sia a livello di programma applicativo;
- assegnazione e utilizzo delle user-id su base strettamente personale e non di gruppo;
- censimento periodico delle user-id esistenti, dei soggetti ai quali tali user-id sono state inizialmente assegnate e dei soggetti che effettivamente le utilizzano
- possibilità di individuare e rimuovere periodicamente le vulnerabilità e le configurazioni poco sicure a livello applicativo e di sistema operativo;
- certificazioni di conformità ai sensi art. 25 del Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003) rilasciate regolarmente da fornitori e installatori, sia in occasione della prima installazione e configurazione, sia in occasione di qualsiasi intervento successivo;
- protezione adeguata da virus e codici maligni;
- protezione perimetrale adeguata in caso di apertura, anche temporanea, ad Internet.

Art. 23 - Verifica periodica dei requisiti minimi sugli strumenti elettronici, informatici e telematici e delle misure minime di sicurezza

I requisiti minimi di cui al punto precedente, e più in generale le misure minime previste dagli artt. 33, 34 e 35 del D.Lgs. 196/2003 nei modi previsti dal Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003) dovranno essere verificati periodicamente con frequenza almeno annuale, da riportare nel Documento programmatico sulla sicurezza, mediante verifiche in loco dei locali, degli apparati e dei programmi, effettuando un'accurata analisi dei rischi e individuando le non conformità e le azioni correttive da mettere in atto.

Periodicamente si dovrà inoltre verificare che le misure pianificate siano state messe in atto, e il livello effettivo di efficacia delle misure stesse. Di tutto quanto appena elencato si dovrà redigere apposita relazione da discutere periodicamente con il Responsabile del trattamento dei dati.

Art. 24 - Notificazione al Garante per la protezione dei dati personali

Stanti le finalità individuate all'art. 5, non è necessario che i trattamenti di dati disciplinati nel presente regolamento siano notificati al Garante per la protezione dei dati personali, in quanto sono richiamati all'interno del Provvedimento del 31 marzo 2004, pubblicato in G.U. n. 81 del 6 aprile 2004, avente ad oggetto i trattamenti sottratti all'obbligo di notificazione. Tuttavia, al titolare viene data la facoltà in qualsiasi caso di effettuare la notifica (che comporterà però il pagamento di Euro 150,00 per diritti di segreteria), soprattutto laddove dovessero mutare in futuro alcuni elementi significativi.

Art. 25 - Inventario delle telecamere installate

Si dovrà tenere un inventario delle telecamere installate, da aggiornare periodicamente e in ogni caso ogniqualvolta venga installata una nuova telecamera (o ne venga sostituita una già installata). Detto inventario, depositato agli atti del Responsabile del servizio, dovrà riportare le seguenti informazioni:

- luogo/località di installazione delle telecamere
- numero di telecamere installate
- finalità principali di installazione delle telecamere
- caratteristiche tecniche principali delle telecamere installate.

Art. 26 - Verifica preliminare da parte del Garante e valutazione di Impatto per la protezione dei dati personali

Sicurezza dei dati

Al momento attuale non è necessaria la verifica preliminare da parte del Garante per le protezione dei dati personali, in quanto la suddetta verifica preliminare è necessaria solo ed esclusivamente nei casi indicati puntualmente all'interno del provvedimento del 29 aprile 2004 del Garante per le protezione dei dati personali.

In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), RGPD, qualora il trattamento di dati realizzato mediante il sistema di videosorveglianza comunale dia luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, l'Ente procederà ad una valutazione di impatto sulla protezione dei dati personali.

Parimenti si procederà nei casi in cui, il trattamento di dati realizzato mediante il sistema di videosorveglianza presenti un rischio comunque elevato per i diritti e le libertà delle persone fisiche.

In questa fase di prima attuazione della normativa europea, l'Ente, in conformità al disposto di cui all'art. 35, Paragrafi 4 e 5, RGPD, al fine di avere maggiore chiarezza in relazione ai nuovi adempimenti, attenderà la pubblicazione obbligatoria da parte dell'Autorità Garante per la protezione dei dati personali dell'elenco delle tipologie di trattamenti soggetti alla Valutazione di impatto e l'eventuale pubblicazione dell'elenco delle tipologie di trattamenti per le quali non è richiesta una Valutazione di impatto.

I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente

I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:

a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

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

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

Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Amministrazione terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ente.

A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi privilegi di visibilità e di trattamento delle immagini. Tenendo conto dello stato dell'arte ed in base alle caratteristiche dei sistemi utilizzati, i soggetti designati quali responsabili e incaricati del trattamento, dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti a ciascuno, unicamente le operazioni di competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime immagini operazioni di cancellazione o di duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 10, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
d) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele; in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
e) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;

f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie Wi–Fi, Wi Max, Gprs).

Come già indicato al precedente art. 8, il titolare del trattamento procede a designare con atto scritto il Responsabile del trattamento dei dati e, quest'ultimo, come già indicato all'art. 9, provvede ad individuare, sempre in forma scritta, le persone fisiche incaricate del trattamento, autorizzate ad accedere ai locali dove sono situate le postazioni di controllo, ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Il Titolare ed il Responsabile del trattamento vigilano sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvedono altresì ad istruire e formare gli incaricati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

Art. 27 - Autorizzazione da parte del Garante per la protezione dei dati personali

Al momento attuale non è necessaria l'autorizzazione da parte del Garante per la protezione dei dati personali, in quanto tale autorizzazione è necessaria solo nel caso di trattamento di dati sensibili e giudiziari (es. riprese di persone malate o di detenuti).

Art. 28 - Cessazione del trattamento

In caso di cessazione del trattamento, i dati dovranno essere distrutti, ad eccezione di quelli per i quali siano in corso o vi siano state in passato richieste di estrazione, che dovranno essere conservati a cura del titolare per fini di documentazione e riscontro.

Art. 29 - Limiti alla utilizzabilità dei dati personali

La materia è disciplinata dall'art. 14 del D.Lgs. 196/2003.

Art. 30 - Danni cagionati per effetto del trattamento dei dati personali

La materia è disciplinata dall'art. 15 del D.Lgs. 196/2003: chiunque cagiona danni per effetto del trattamento dei dati personali è tenuto al risarcimento dei danni causati, ai sensi dell'art. 2050 del Codice Civile (**Responsabilità per l'esercizio di attività pericolose**: *chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee ad evitare il danno*).

Quanto sopra riportato significa che il trattamento di immagini è considerato attività inerentemente pericolosa, per lo svolgimento della quale sarà necessario adottare non solo tutte le misure minime di sicurezza previste dagli artt. 31, 32, 33, 34 e 35 del D.Lgs. 196/2003 nei modi previsti dal Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003), ma tutte quelle ritenute idonee e necessarie, a fronte di una analisi dei rischi da effettuarsi con frequenza almeno annuale, a prevenire o limitare il danno.

Art. 31 - Comunicazione

La comunicazione di dati personali da parte del titolare ad altri soggetti pubblici è ammessa quando è prevista da norma di legge o di regolamento attuativo di norma di legge, oppure quando risulti comunque necessaria per lo svolgimento delle funzioni istituzionali.

La comunicazione di dati personali da parte del titolare a privati o ad enti pubblici economici è ammessa unicamente quando prevista da norma di legge o di regolamento.

Art. 32 - Tutela amministrativa e giurisdizionale

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, RGPD ed alle previsioni che saranno contenute nel Decreto Legislativo di prossima emanazione recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, 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", in attuazione della delega al Governo di cui all'art. 13, L. 163/2017.

Art. 33 - Modifiche e integrazioni regolamentari

Il presente regolamento dovrà essere adeguato per recepire eventuali modifiche alla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento alle disposizioni e ai provvedimenti emanati dal Garante per la protezione dei dati personali.

Inoltre, il presente regolamento dovrà venire modificato nel caso dovessero mutare le finalità del sistema di videosorveglianza.

Art. 34 - Norme finali

Per quanto non disciplinato dal presente regolamento, si rinvia al Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003, n. 196), e al provvedimento generale sulla videosorveglianza emesso dal Garante per la protezione dei dati personali il 29 aprile 2004.

Art. 35 - Pubblicità e conoscibilità del regolamento

Il regime di eventuale pubblicità e conoscibilità del presente regolamento è disciplinato dallo Statuto del Comune di Ciconio e dalla disciplina rilevante in materia di accesso agli atti e documenti amministrativi.
Il presente regolamento verrà pubblicato sul Sito del Comune di Ciconio, come prescritto dalla norma.

Art. 36 - Impianto sanzionatorio

Sono incaricati a vigilare sul rispetto delle norme contenute nel presente regolamento e di procedere all'accertamento delle relative violazioni gli agenti della Polizia Municipale.

Il personale indicato nel comma precedente può identificare, anche attraverso la richiesta di esibizione di documenti, coloro che pongono in essere condotte vietate dalla legge e dal presente regolamento e redigere verbale sulle infrazioni rilevate.

Per l'accertamento delle violazioni, la contestazione, la notificazione delle medesime, la definizione degli accertamenti, l'individuazione dell' organo competente ad irrogare le sanzioni, l'irrogazione delle medesime e la devoluzione dei proventi delle somme riscosse si osservano le norme della legge di depenalizzazione 689/1981.

E' ammesso il pagamento di una somma in misura ridotta pari alla terza parte del massimo della sanzione prevista per la violazione commessa o, se più favorevole e qualora sia stabilito il minimo della sanzione edittale, pari al doppio del relativo importo, oltre alle spese del procedimento, entro il termine di sessanta giorni dalla contestazione immediata o, se questa non vi è stata, dalla notificazione degli estremi della violazione.

L'impianto sanzionatorio farà riferimento alla normativa vigente al momento della contestazione, oltre a quanto stabilito dal D. Lgs. 196/2003 ("Codice Privacy") e dal Regolamento UE n. 2016/679 ("General Data Protection Regulation 2016/679") per la quantificazione delle ammende comminabili in caso di violazioni al presente regolamento o alla normativa cogente e vigente.

Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82, RGPD.

Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

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.

Art. 37 – Entrata in vigore

Il presente regolamento entrerà in vigore decorsi 15 giorni dalla pubblicazione sull'Albo Pretorio Comunale.