REGOLAMENTO PER LA DISCIPLINA DEL SISTEMA DI VIDEOSORVEGLIANZA NEL COMUNE DI STAZZEMA

AGGIORNATO CON: LA LEGGE N° 38 DEL 23 APRILE 2009 IL PROVVEDIMENTO DEL GARANTE DELLA PRIVACY DELL' 8 APRILE 2010 LA DIRETTIVA DEL MINISTERO DELL'INTERNO DEL 02.03.2012

(approvato con deliberazione del Consiglio Comunale N° 56 del 27/10/2015)

SOMMARIO

1 PREMESSA

Il presente Regolamento disciplina l'utilizzo del sistema di videosorveglianza sul territorio per il controllo urbano a copertura delle vie di accesso del Comune di Stazzema. Recepisce le nuove disposizioni del Provvedimento Generale del Garante della Privacy dell'8 aprile 2010, confermative delle prescrizioni contenute nell'art. 6 commi 7/8 della Legge 23 aprile 2009 n° 38, riguardanti finalità e trattamento dei dati, nonché la Direttiva del Ministero dell'Interno del 02 marzo 2012. Con tale regolamento viene garantito il trattamento dei dati personali, nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dei cittadini, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione degli stessi. Vengono parimente garantiti i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento. Per tutto quanto non dettagliatamente disciplinato nel presente regolamento si rinvia alle disposizioni del Codice in materia di protezione dei dati personali, approvato con Decreto Legislativo 30 giugno 2003, n. 196.

2 DEFINIZIONI

Ai fini del presente documento si intende per:

"trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

"dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

"dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

"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;

"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;

"titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

"responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

"incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

"interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

"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;

"diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

"blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

"banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

"garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

"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;

"strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"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;

"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;

"profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

"sistema di 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.

3 AMBITO DI APPLICAZIONE DEL DOCUMENTO

Il presente regolamento disciplina il trattamento dei dati ottenuti mediante l'impianto di videosorveglianza attiva presso il Comune di Stazzema e precisamente nelle seguenti zone:

- Loc. Iacco (SP9)
- Pubblica Assistenza (SP1)
- Arni

4 NORMATIVA DI RIFERIMENTO

Il presente regolamento è conforme al Provvedimento Generale del Garante per la Privacy dell' 08 aprile 2010, alla Legge 23 Aprile 2009 n° 38, alla disciplina generale in materia di protezione dei dati personali prevista dal D. Lgs. 196/2003, alle Circolari del Capo della Polizia n. 558/A421.2/70/456 dell'8 febbraio 2005 e n. 558/A/421.2/70/195960 del 6 agosto 2010, adottato nel rispetto della Legge n. 65 del 07 marzo 1986 (legge-quadro sull'ordinamento di Polizia Municipale) e successive modificazioni e alle specifiche Leggi regionali di settore. Recepisce altresì la direttiva del Ministero dell'Interno datata 02 marzo 2012. Per quanto non espressamente previsto dal presente documento si rinvia alla normativa di riferimento.

5 SCOPO DEL SISTEMA DI VIDEOSORVEGLIANZA

La sicurezza rappresenta un bene primario verso il quale la popolazione manifesta un grande interesse e forti aspettative. Non è solo ordine e sicurezza pubblica ma oggi anche sicurezza partecipata ed integrata, in cui ogni possibile strumento, ogni risorsa, concorre al mantenimento di una ordinata e civile convivenza, alla vivibilità delle nostre città. Il Comune di Stazzema utilizza l'impianto di videosorveglianza per sopperire alle esigenze di sicurezza e di ordine pubblico ordinarie e straordinarie. Nello specifico in riferimento allo svolgimento di manifestazioni, il tutto in orari diurni e notturni, in presenza di personale addetto al controllo o meno a salvaguardia della sicurezza dei cittadini, del patrimonio del Comune, del controllo del territorio, anche in una visione allargata di tutela della sicurezza urbana.

In modo particolare si precisa quanto segue.

1. Le finalità del suddetto impianto sono del tutto conformi alle funzioni istituzionali demandate al Comune di Stazzema dal D.Lgs. 18/08/2000 n.267 e dal DPR 24/07/1977 n.616 e dalla L. 07/03/86 n.65 sull'ordinamento della Polizia Locale e dai Regolamenti Comunali vigenti, e che in via puramente esemplificativa sono:

   - l'attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale;

   - la ricostruzione, in tempo reale, della dinamica di atti vandalici od azioni di teppismo nei luoghi pubblici di principale frequentazione, per permettere un pronto intervento della Polizia Locale e delle Forze dell'Ordine a tutela del patrimonio pubblico;

- la verifica, il controllo e la gestione dell'accesso a zone a traffico limitato; la rilevazione ed il controllo di mezzi non in regola con gli obblighi di legge.
- l'attivazione di uno strumento operativo di protezione civile sul territorio comunale.

2. La disponibilità tempestiva di immagini a disposizione della Polizia Locale costituisce, inoltre, uno strumento di controllo urbano a copertura delle vie di accesso al Comune e di razionalizzazione dell'azione delle pattuglie della Polizia Locale, in modo particolare:
   - il controllo di parte del centro urbano di Stazzema e di alcune aree comunali ritenute di particolare interesse;
   - prevenire 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" così individuata secondo il Decreto del Ministero dell'Interno 5 agosto 2008;
   - rilevare situazioni di pericolo per la sicurezza pubblica, consentendo l'intervento degli operatori;
   - agevolare il controllo e le verifiche sulla tipologia e numero di mezzi pesanti ed in modo particolare dei mezzi destinati al trasporto dei materiali lapidei.

6 RISPETTO DEI PRINCIPI GENERALI DEL PROVVEDIMENTO DEL GARANTE DELL' 08.04.2010

I soggetti pubblici, in qualità di titolari del trattamento (art. 4, comma 1, lett. f), del Codice), possono trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (art. 11, comma 1, lett. b), del Codice), soltanto per lo svolgimento delle proprie funzioni istituzionali. Ciò vale anche in relazione a rilevazioni di immagini mediante sistemi di videosorveglianza (art. 18, comma 2, del Codice).

6.1 RISPETTO DEL PRINCIPIO DI LICEITÀ

Il trattamento di dati raccolti attraverso il sistema di videosorveglianza è possibile solo se fondato su uno dei presupposti di legalità previsti dal Codice della Privacy e deve essere effettuato nel rispetto delle prescrizioni stabilite dalla normativa in materia di protezione di dati personali, ovvero nello svolgimento di funzioni istituzionali.

Il sistema è installato esclusivamente per le finalità di cui al precedente art. 5. La videosorveglianza, inoltre, nel caso di specie, avviene nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di Legge da osservare in caso di installazione di apparecchi audiovisivi: le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela, le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (Statuto dei lavoratori). E' garantito il rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni.

6.2 RISPETTO DEL PRINCIPIO DI NECESSITÀ

Per il principio di necessità, il sistema informativo e il relativo programma informatico sono conformati in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi ed il software è configurato in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati con le modalità di cui al successivo art. 8.3.

6.3 RISPETTO DEL PRINCIPIO DI PROPORZIONALITÀ

Il principio di proporzionalità impone che l'uso di telecamere è lecito solo quando altre misure di sicurezza siano ritenute insufficienti o inattuabili. La videosorveglianza deve costituire l'estrema ratio, utilizzabile solo laddove altri sistemi quali allarmi, controlli da parte degli addetti, misure di protezione degli ingressi ecc., risultino insufficienti. Oltre a ciò dovrà essere evitata l'acquisizione di dati in aree che non sono soggette a concreto pericolo, i dati non devono essere eccedenti rispetto alle finalità e devono essere conservati solo per il tempo necessario in relazione ai quali sono raccolti e trattati.

6.4 RISPETTO DEL PRINCIPIO DI FINALITÀ

Per Il principio di finalità il titolare del trattamento può perseguire con la videosorveglianza solo finalità di sua pertinenza, esclusivamente per scopi determinati, espliciti e legittimi.

Queste finalità sono determinate e rese trasparenti, direttamente conoscibili attraverso adeguati cartelli di avvertimento al pubblico e riportate nell'informativa pubblicata sul sito del Comune.

7 RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Il Comandante della Polizia Municipale in servizio o il suo sostituto, ai sensi della vigente organizzazione del Corpo, è designato quale Responsabile del trattamento dei dati personali rilevati, ai sensi e per gli effetti dell'art. 1," lett. e." Lo stesso sarà designato con atto del Sindaco.

Il Responsabile designa per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le apparecchiature di archiviazione dei dati, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Il Responsabile provvede altresì ad individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni quali la registrazione, la copia, la cancellazione, la modifica dello zoom, ecc.

Gli incaricati andranno nominati tra soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dati; agli stessi saranno affidati compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi, previa istruzione sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento.

Il Responsabile e gli incaricati procedono al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza di quanto disposto dal Regolamento e delle proprie istruzioni.

8 CARATTERISTICHE TECNICHE DEL SISTEMA DI VIDEOSORVEGLIANZA

8.1 NUMERO DI TELECAMERE

Si riportano di seguito i dati relativi a ciascun sito oggetto di installazione delle telecamere:

Vie di accesso al territorio comunale			
Riferimento	***Denominazione***	***N. telecamere controllo targhe***	***N. telecamere di contesto***
S1	Loc. Iacco	1	3+1(integrata nella telecamera di controllo targhe)
S2	Pubblica Assistenza (sede)	1	1(integrata nella telecamera di controllo targhe)
S3	Arni	1	1(integrata nella telecamera di controllo targhe)
	Totale	**3**	**6**

Tale sistema, senza necessità di modificare il presente Regolamento, potrà essere ulteriormente implementato, secondo le necessità e le esigenze future, nel rispetto del Provvedimento Generale del Garante della Privacy dell'8 aprile 2010, nonché della Direttiva del Ministero dell'Interno del 02 marzo 2012. Gli apparati acquistati ed installati dal Comune sono e saranno gestiti direttamente dalla Polizia Municipale.

8.2 TIPOLOGIE DI TELECAMERE INSTALLATE

Le telecamere installate nei singoli punti o zone di rilevamento sono di tipologie "videocamere fisse".

8.3 TEMPO DI CONSERVAZIONE DELLE IMMAGINI

In applicazione del principio di proporzionalità le immagini vengono conservare per un periodo massimo di 7 giorni successivi alla rilevazione delle informazioni e delle immagini raccolte, dopodiché vengono automaticamente cancellate dal sistema informatico.

8.4 CENTRO DI GESTIONE ED ARCHIVIAZIONE

Le apparecchiature informatiche che si occupano della gestione ed archiviazione dei dati acquisiti dal sistema di videosorveglianza sono installate entro il locale CED ad accesso controllato presente nel Palazzo Comunale di Stazzema. Il locale è dotato di serratura a chiave di sicurezza.

I dati sono tutti trattati, gestiti ed archiviati in formato digitale, in modo particolare si precisa che i dati relativi alle targhe degli automezzi che transitano i varchi devono essere memorizzate su pc

configurato in modalità server dotato di due hard disk tipo SSD[1] configurati in raid[2] 1 mentre i flussi video e le immagini di contesto devono essere archiviate su NAS[3] dotato di n.4 hard disk configurati in raid 5.

L'accesso a queste due banche dati deve avvenire impiegando software distinti dotati entrambi di sistemi di autenticazione basati su parole chiavi che consentono l'individuazione dell'incaricato che accede al sistema e l'assegnazione delle autorizzazioni associate al suo incarico, ciò in modo del tutto automatico e trasparente per l'operatore.

8.5 MODALITÀ DI RACCOLTA DATI E REQUISITI DEI DATI PERSONALI

1. I dati personali oggetto di trattamento sono:
    a. trattati in modo lecito e secondo correttezza;
    b. raccolti e registrati per le finalità di cui al precedente art. 6.4 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi, esatti e, se necessario, aggiornati;
    c. raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
    d. conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito al precedente comma 8.3;
    e. trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, di cui al precedente art. 5, con modalità volta a salvaguardare l'anonimato ed in ogni caso successivamente alla fase della raccolta, atteso che le immagini registrate possono contenere dati di carattere personale.
2. La localizzazione dei punti di ripresa delle telecamere dell'impianto di videosorveglianza installate sul territorio comunale in corrispondenza di incroci, vie d'accesso ed uscita dall'abitato, piazze, parchi, immobili pubblici ed altri luoghi, sono rinvenibili nell'elenco dei siti di ripresa all'uopo predisposto ed aggiornato (Allegato n.1) . Alle modifiche e/o integrazioni di detto elenco, provvederà di volta in volta la Giunta con relativo atto di recepimento.
3. Le telecamere indicate come di 'contesto' di cui al precedente comma 8.1 consentono, tecnicamente, riprese video a colori o in bianco e nero; sono dotate di zoom digitale; le telecamere indicate come 'lettura targhe' sono apparati in grado di rilevare le targhe dei veicoli in transito, sono videocamere munite di infrarosso impulsato e consentono il riconoscimento delle targhe con un sistema di rilevamento automatico dei caratteri (OCR[4])

[1] Solid State Disk (SSD) - hard disk di ultima generazione caratterizzati da essere dispositivi di memorizzazione allo stato solido, non avere parti in movimento e quindi avere velocità di accesso ai dati in lettura e scrittura molto più rapidi rispetto ad un normale hard disk.
[2] Redundant Array of Independent Disks (RAIS) - si tratta di un dispositivo hardware che riunisce tra loro un insieme ridondante di dischi indipendenti, è una tecnica di raggruppamento di diversi dischi rigidi che li rende utilizzabili come se fossero un unico volume di memorizzazione. Tale aggregazione sfrutta, con modalità differenti a seconda del tipo di implementazione, i principi di ridondanza dei dati e di parallelismo nel loro accesso per garantire, rispetto ad un disco singolo, incrementi di prestazioni, aumenti nella capacità di memorizzazione disponibile, miglioramenti nella tolleranza ai guasti.
[3] Network Attached Disk (NAS) - è un dispositivo collegato ad una rete di computer la cui funzione è quella di condividere tra gli utenti della rete una memoria di massa costituita da più hard disk.
[4] Optical Character Recognition (OCR) – software dedicato alla conversione di un'immagine contenente testo

implementato a bordo camera; quelle mobili sono brandeggianti (in verticale e in orizzontale).
Tutti gli apparati sono collegati al centro di gestione ed archiviazione di cui al comma 8.4, tutti i dati sono acquisiti dalle telecamere, trasmessi dai ponti radio e dai ponti 3G, archiviati e gestiti in modalità esclusivamente digitale consentendo un elevato grado di precisione, minima perdita di informazioni ed un elevatissimo dettaglio delle riprese.
Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali. Le telecamere per la rilevazione delle targhe, che sfruttano la tecnologia OCR, vengono utilizzate per l'esclusiva finalità di tutela della sicurezza urbana e saranno installate in ossequio alla direttiva del Ministero degli Interni del 2 marzo 2012.
Le immagini riprese dalle telecamere tradizionali sono visibili in tempo reale ad una risoluzione tale da garantire la riservatezza e tutela dei dati, solamente nella fase di interrogazione le riprese diventano visibili alla massima risoluzione programmata, ottemperando in tal modo all'esigenza di riservatezza e tutela dei dati.
Le immagini riprese dalle telecamere dotate di sistema OCR a bordo, sono visibili in tempo reale ma solo ed unicamente tramite opportuno software di interrogazione che consente all'incaricato di ricevere le informazioni necessarie all'espletamento delle finalità di cui all'art. 5 del Regolamento.

9 MISURE DI SICUREZZA

Il sistema verrà installato adottando le misure di sicurezza volte a ridurre i rischi di distruzione, perdita, anche accidentale delle informazioni, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta dei dati relativi alla videosorveglianza.

9.1 SICUREZZA FISICA

Gli accessi ai sistemi di visione e rilevazioni sono selezionati. L'accesso del personale autorizzato al trattamento dei dati avviene, solitamente, durante l'orario di lavoro dell'ente. In casi eccezionali e per motivi esclusivamente istituzionali è consentito l'accesso anche al di fuori dei giorni stabiliti e dell'orario fissato. In generale i documenti contenenti dati personali sensibili sono custoditi in armadi o cassetti chiusi a chiave o in caso comunque di allontanamento anche momentaneo dal proprio Ufficio di tutti i dipendenti.

9.2 MISURE PER PREVENIRE RISCHI DIPENDENTI DA COMPORTAMENTI DEGLI OPERATORI

I rischi dipendenti da comportamenti dei soggetti incaricati dei trattamenti sono contrastati da misure di informazione e formazione degli operatori. Tutto il personale deve essere informato e deve ricevere le regole di corretta gestione dei dati personali. Sarà periodicamente verificata la corretta gestione e conservazione delle credenziali di autenticazione. I comportamenti fraudolenti sono perseguiti con le consuete misure di carattere disciplinare e prevenuti da attività di verifica e controllo riservata a ciascun Responsabile in riferimento agli operatori del Settore. I possibili errori materiali sono prevenuti da criteri procedurali che prevedono controlli e verifiche.

9.3 TRATTAMENTI INFORMATICI

1. Funzione di autenticazione e gestione delle password

- Il trattamento di dati personali con strumenti elettronici è consentito solo ai titolari dotati di credenziali di autenticazione che consentano il superamento di una procedura di verifica relativa a uno specifico trattamento o ad un insieme di trattamenti.
- Le credenziali di autenticazione stabilite e previste consistono in un codice per l'identificazione di ciascun incaricato associato a una parola chiave, riservata, conosciuta solamente dal medesimo e dall'amministratore di sistema.
- Sono attribuite una o più credenziali per l'autenticazione e l'accesso ai vari programmi.
- Agli incaricati sono impartite le dovute istruzioni affinché ciascuno adotti le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso e di uso esclusivo.
- Ciascuna parola chiave prevista dovrà essere, di norma, composta da almeno otto caratteri alfanumerici. Nel caso in cui lo strumento elettronico non lo permetta, la parola chiave sarà composta da un numero di caratteri pari al massimo consentito. Essa non potrà contenere riferimenti agevolmente riconducibili all'incaricato e dovrà essere modificata da quest'ultimo almeno ogni sei mesi.
- In caso di prolungata assenza o impedimento dell'incaricato (malattia/ferie/ecc.) che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il titolare e/o il responsabile potrà assicurare la disponibilità di dati o strumenti elettronici previa richiesta dell'incaricato che necessita tale disponibilità.
- Gli incaricati devono essere avvertiti di non lasciare incustodito e accessibile lo strumento elettronico fisso o portatile impiegato per l'interrogazione dei dati durante una sessione di trattamento.
- Il codice d'identificazione personale non deve essere comunicato né assegnato ad altri incaricati.
- Le credenziali di autenticazione non utilizzate da almeno sei mesi saranno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- Le credenziali saranno disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

2. Sistema di autorizzazione
   - Per gli incaricati devono essere individuati profili di autorizzazione a livelli differenziati a seconda della specifica abilitazione al trattamento dati.
   - I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
   - Gli utenti sono diversificati a seconda del profilo: ad esempio consultazione, consultazione ed elaborazione, accesso totale (amministratore di sistema), manutenzione ed assistenza tecnica.
   - Periodicamente, e comunque almeno annualmente, sarà verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
   - La gestione di autenticazione e profili per ogni singolo incaricato viene valutata dal Responsabile settore informatico in base alle necessità che il singolo incaricato ha di accedere ai dati per lo svolgimento delle funzioni e dei compiti che gli sono affidati.
3. Log degli eventi

L'accesso ai vari sistemi software viene registrato all'interno del sistema informatico, le registrazioni avvengono in modo cronologico e consentono al Responsabile del trattamento dei dati personali l'analisi delle operazioni eseguite e dei soggetti che le hanno effettuate.

9.4 CAUTELE E COMPORTAMENTI DA ADOTTARE

1. I dispositivi di visualizzazione impiegati per la visione delle immagini, la consultazione ed interrogazione dei dati acquisiti dal sistema devono essere posizionati e gestiti dagli operatori in modo tale da non permetterne la visione, neanche occasionalmente, a persone estranee non autorizzate.
2. L'accesso alle immagini da parte del responsabile e degli incaricati del trattamento deve limitarsi alle attività oggetto di videosorveglianza; eventuali altre informazioni di cui questi vengono a conoscenza, mentre osservano il comportamento di un soggetto ripreso, devono essere ignorate.
3. Nel caso le immagini siano conservate per una specifica richiesta investigativa dell'autorità giudiziaria o di un organo di polizia giudiziaria, i relativi supporti di memorizzazione (CD/DVD/HD/SD o altri) devono essere custoditi in un armadio (o simile struttura) dotato di serratura, apribile solo dal Responsabile e dagli incaricati del trattamento.
4. La cancellazione dei dati deve avvenire preferibilmente mediante il nuovo utilizzo del supporto e cioè sovrascrivendo i dati con altre informazioni anziché tramite semplice cancellazione e/o formattazione del supporto; comunque le operazioni di cancellazione dovranno essere effettuate sul luogo di lavoro.
5. Nel caso in cui il supporto debba essere sostituito per eccessiva usura, dovrà essere distrutto in modo che non possa essere più utilizzabile, né che possano essere recuperati dati in esso presenti.
6. L'accesso ai dati è consentito solo ai seguenti soggetti:
    a. al Titolare del trattamento;
    b. al Responsabile ed agli incaricati dello specifico trattamento;
    c. per indagini delle Autorità giudiziarie o di Polizia;
    d. all'Amministratore del sistema, individuato dalla ditta incaricata della manutenzione degli impianti;
    e. al terzo, debitamente autorizzato, in quanto oggetto delle riprese.
7. Nel caso di accesso alle immagini per indagine delle autorità giudiziarie o di polizia occorrerà comunque l'autorizzazione da parte del Responsabile del Trattamento o del Titolare.
8. Nel caso di accesso alle immagini del terzo, debitamente autorizzato, questi dovrà avere visione solo delle immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà essere utilizzata, da parte dell'incaricato al trattamento, una schermatura del video, tramite opportune accortezze.

10 CARTELLI DI AVVERTIMENTO ED INFORMATIVA AI CITTADINI

I cittadini devono essere opportunamente informati della presenza della zona di videosorveglianza per il tramite di apposita cartellonistica conforme ai dettami previsti dal

Garante. Sul territorio comunale devono essere collocati cartelli di avvertimenti al pubblico, identici a quello riportato in Allegato n.2.

Il supporto con l'informativa, in particolare, deve essere installato all'ingresso delle aree sottoposte a videosorveglianza ed i cartelli devono essere previsti per formato e collocazione in modo tale da essere chiaramente visibili.

11 RESPONSABILI ED INCARICATI DEL TRATTAMENTO E PERSONE AUTORIZZATE AD ACCEDERE AL SISTEMA

Devono essere designate per iscritto le persone fisiche incaricate al trattamento dei dati, autorizzate all'accesso degli impianti secondo le rispettive credenziali. I soggetti, a cui è consentita l'estrapolazione delle informazioni e delle immagini, vengono individuati con successivo atto del Responsabile. Sono previsti livelli di accesso al sistema specifici per l'utilizzo delle informazioni, avuto riguardo anche ad eventuali interventi per esigenze di manutenzione. Il personale deve essere responsabilizzato affinché siano evitati rischi specifici nell'ambito dell'attività di ciascuno.

12 NOMINA A RESPONSABILE ESTERNO PRIVACY ED ATTESTAZIONE DI CONFORMITÀ PER INTERVENTI TECNICI SUL SISTEMA DI INFOMIBILITA' E VIDEOSORVEGLIANZA

Il Responsabile di Servizio, qualora si rendesse necessario un intervento sul sistema informatico, potrà avvalersi di personale esterno nominato a seguito di procedura ad evidenza pubblica.

In particolare il soggetto cui le attività sono affidate dovrà:

1. essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
4. impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate. La sostituzione dell'amministratore di sistema dovrà avvenire con atto separato del Titolare del trattamento dei dati. La Polizia Municipale si impegna inoltre, in caso di interventi tecnici per la manutenzione del sistema informatico relativo alla videosorveglianza, a richiedere e pretendere dall'installatore un documento dettagliato circa l'intervento effettuato e la sua conformità alle disposizioni del disciplinare tecnico del Codice della Privacy.

13 NOTIFICAZIONE PREVENTIVA AL GARANTE

1. I dati trattati devono essere notificati al Garante solo se rientrano nei casi specificatamente previsti dalla normativa vigente sulla privacy. A tale proposito la normativa prevede che non vadano comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardino immagini conservate temporaneamente per esclusive finalità di sicurezza pubblica o di tutela delle persone e del patrimonio.
2. I sistemi di lettura targhe abbinate a banca dati dei proprietari dei veicoli non rientrano tra gli esempi citati nel provvedimento dell'8 aprile 2010 né per quanto riguarda l'obbligo di verifica preliminare, né per quanto concerne la sicura esclusione da tale obbligo. Non è necessaria la verifica preliminare del Garante se i sistemi di videosorveglianza si limitano a una lettura delle targhe, senza altre associazioni con altri dati tali da provocare pregiudizio per gli interessati; di conseguenza non deve essere adempiuto l'obbligo previsto dall'art. 17 del Codice. L'obbligo di verifica preliminare ricorre quando l'associazione delle immagini avvenga con altri particolari dati (quali sono i dati biometrici o dati sensibili) e non con qualsiasi tipologia di dato personale. Per l'assenza dell'obbligo della verifica preliminare si è espresso anche l'ANCI in "Linee guida in materia di videosorveglianza". Pertanto anche il sistema di lettura targhe implementato non è soggetto ad alcuna verifica preliminare e tantomeno deve essere segnato da comunicazione al Garante della privacy

14 PROCEDURA PER L'ACCESSO ALLE IMMAGINI DA PARTE DI TERZI

1. La persona interessata ad accedere alle immagini deve avanzare apposita istanza (fac-simile viene riportato in Allegato 3) al Responsabile del trattamento, indicato nell'informativa e dovrà in essa essere indicato a quale impianto di videosorveglianza si fa riferimento e dovrà essere indirizzata all'Ufficio Protocollo del Comune di Stazzema.
2. Nel caso le immagini di possibile interesse non siano oggetto di conservazione, di ciò dovrà essere data formale comunicazione al richiedente.
3. Nel caso le immagini di possibile interesse siano oggetto di conservazione, il richiedente dovrà fornire altresì ulteriori indicazioni, finalizzate a facilitare il reperimento delle immagini stesse, tra cui:
    a. il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa;
    b. il luogo ed i luoghi di possibile ripresa;
    c. la presenza di altre persone,;
    d. una descrizione dell'attività svolta durante le riprese.
4. Nel caso che tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data comunicazione al richiedente.
5. 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 il suddetto potrà visionare le immagini che lo riguardano.
6. Nel caso il richiedente intenda sporgere reclamo, dovrà presentare apposita istanza (fac-simile viene riportato in Allegato 4), indirizzata al Responsabile del trattamento, indicando i motivi del reclamo.

15 MODIFICHE

1. Il presente regolamento si aggiorna senza necessità di espressa modifica qualora dovessero intervenire modifiche normative o regolamentari in materia di videosorveglianza e trattamento dei dati personali.
2. Dovrà essere aggiornato ovvero in caso di variazione dell'assetto territoriale dell'Ente.
3. La competenza a decidere sull'implementazione degli apparati e loro collocazione, ed alle conseguenti modifiche ed integrazioni al prospetto di cui all'art. 8 ed all'elenco allegato n. 1, viene attribuita alla Giunta Comunale.

ALLEGATO N.1 – ELENCO DEI SITI DI RIPRESA E COLLOCAZIONE

Aggiornato a XXXX 2015

Vie di accesso al territorio comunale			
Riferimento	***Denominazione***	***N. telecamere controllo targhe***	***N. telecamere di contesto***
S1	Loc. Iacco	1	3+1(integrata nella telecamera di controllo targhe)
S2	Pubblica Assistenza (sede)	1	1(integrata nella telecamera di controllo targhe)
S3	Arni	1	1(integrata nella telecamera di controllo targhe)
	Totale	**3**	**6**

ALLEGATO N.2 – ELENCO DEI SITI DI RIPRESA E COLLOCAZIONE

ALLEGATO N.3 – FAC-SIMILE RICHIESTA DI ACCESSO

Il/La sottoscritto/a …… identificato tramite …… ai sensi della vigente normativa in materia di privacy richiede di esercitare il diritto di accesso alle immagini video che potrebbero aver registrato dati personali a se stesso afferenti.

Per permette di individuare tali immagini nell'archivio video, fornisce le seguenti informazioni:

1. Luogo o luoghi di possibile ripresa
   ……
2. Data di possibile ripresa ……
3. Fascia oraria di possibile ripresa (approssimazione di 30 minuti) ……
4. Abbigliamento al momento della possibile ripresa
   ……
5. Accessori indossati (borse, ombrelli, animali al guinsaglio ed ogni altra informazione utile all'identificazione del soggetto)
   ……
6. Presenza di accompagnatori (indicare numero, sesso e descrizione sommaria)
   ……
7. Attività svolta durante la ripresa
   ……

Il/La sottoscritto/a fornisce il seguente recapito e/o contatto telefonico per eventuali contatti ed ulteriori approfondimenti risultassero necessari:

……

Luogo e data

_____

In fede (firma)

_____

PARTE DA CONSEGNARE AL FIRMATARIO DELL'ISTANZA

In data …….. Alle ore …….. Il/La Sig./Sig.a ……

ha avanzato richiesta di accesso al sistema di videosorveglianza ai sensi della vigente normativa in materia di privacy.

Firma del ricevente la richiesta

_____

ALLEGATO N.4 – FAC- SIMILE RECLAMO

Al Responsabile del trattamento dei dati

Comune di Stazzema

Il/La sottoscritto/a …… che aveva presentato in data …….. una richiesta di accesso alle immagini video che potrebbero aver registrato i miei dati personali, presenta reclamo per i seguenti motivi:

……

……

……

……

……

……

……

Il/La sottoscritto/a fornisce il seguente recapito e/o contatto telefonico per eventuali contatti ed ulteriori approfondimenti risultassero necessari:

……

In fede.

Luogo e data

_____

In fede (firma)

_____