

COMUNE DI CAMPO NELL'ELBA
Provincia di Livorno



**REGOLAMENTO PER LA DISCIPLINA
DELLA VIDEOSORVEGLIANZA NEL
TERRITORIO COMUNALE**

Allegato alla Delibera del Consiglio Comunale n. 54 del 20.11.2019

SOMMARIO

Art. 1	Oggetto
Art. 2	Definizioni
Art. 3	Finalità e ambito di applicazione
Art. 4	Principi generali e garanzie
Art. 5	Finalità dell'impianto
Art. 6	Caratteristiche tecniche e Responsabile dell'impianto
Art. 7	Uso delle telecamere
Art. 8	Informativa
Art. 9	Trattamento dei dati personali per finalità istituzionali
Art. 10	Titolare e Responsabile del trattamento
Art. 11	Notificazione
Art. 12	Responsabile della protezione dati RPD
Art. 13	Nomina degli incaricati alla gestione dell'impianto di videosorveglianza
Art. 14	Accertamento di illeciti e indagini di autorità giudiziaria e forze di polizia
Art. 15	Misure di sicurezza e limiti di utilizzo
Art. 16	Trattamento e conservazione dei dati
Art. 17	Modalità di raccolta dei dati
Art. 18	Obblighi degli operatori
Art. 19	Registro unico delle attività di trattamento
Art. 20	Valutazione d'impatto sulla protezione dei dati
Art. 21	Cessazione del trattamento dei dati
Art. 22	Diritti dell'interessato nel trattamento dei dati
Art. 23	Danni cagionati per effetto del trattamento di dati personali
Art. 24	Tutela amministrativa e giurisdizionale
Art. 25	Provvedimenti attuativi
Art. 26	Norma di rinvio
Art. 27	Entrata in vigore

ALLEGATI

- a) Modello per richiesta all'accesso dei locali e visualizzazione immagini in diretta
- b) Modello per richiesta di accesso nei locali per visioni delle immagini videoregistrate
- c) Modello per richiesta di accesso nei locali per eseguire registrazioni delle immagini
- d) Modello per richiedere l'accesso ai locali per manutenzione e verifiche tecniche
- e) Registro degli accessi alla visione delle immagini
- f) Informativa sistema di videosorveglianza del territorio comunale

Art. 1 Oggetto

Il presente regolamento, nel rispetto del principio di proporzionalità tra mezzi impiegati e fini perseguiti, disciplina il trattamento dei dati personali per mezzo di impianti di videosorveglianza del territorio comunale di Campo nell'Elba, determinandone le condizioni necessarie per la tenuta in esercizio ai sensi del D.Lgs 196/03 e s.m., in osservanza delle disposizioni contenute nei codici di deontologia promossi dal Garante con "il decalogo" del 29/11/00 e s.m. e del provvedimento del 29/04/04 e s.m.. Vengono osservate, inoltre, le prescrizioni indicate nel Regolamento Generale sulla protezione dei dati dell'U.E. n. 679/2016 (RGPD) e la Direttiva dell'U.E. n. 680/2016 (Direttiva Polizia), nonché la Direttiva del Ministero dell'Interno n. 558/SICPART/421.2/70/224632 del 02/03/2012.

Art. 2 Definizioni

- a) Per "**banca dati**", il complesso di dati personali, formatosi presso la sala di controllo e trattato esclusivamente mediante riprese videoregistrate che, in relazione ai luoghi di installazione delle videocamere, interessano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto eventuali;
- b) Per "**trattamento**", tutte le operazioni o complesso di operazioni svolte con l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, l'eventuale diffusione, la cancellazione e la distruzione di dati;
- c) Per "**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili anche direttamente, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;
- d) Per "**titolare**", l'Ente Comune di Campo nell'Elba, nelle sue articolazioni interne, competente a disporre per l'adozione ed il funzionamento degli impianti di videosorveglianza ed a cui spettano le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali ed il profilo delle misure di sicurezza per l'utilizzo dei predetti impianti;
- e) Per "**responsabile**", la persona fisica legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento di dati personali;
- f) Per "**incaricati**", le persone fisiche autorizzate dal titolare o dal responsabile a compiere operazioni di trattamento;
- g) Per "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- h) Per "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- i) Per "**diffusione**", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- j) Per "**dato anonimo**", il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- k) Per "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

Art. 3

Finalità e ambito di applicazione

Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono dati personali. La videosorveglianza incide sul diritto delle persone alla propria riservatezza. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza, gestiti ed impiegati dal Comune di Campo nell'Elba nel suo territorio, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza ed all'identità personale. Garantisce, altresì, i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.

Il sistema informativo ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali ed identificativi, in modo da escluderne il trattamento quando le finalità, perseguite nei singoli casi, possano essere realizzate mediante dati anonimi od opportune modalità e che permettano di identificare l'interessato solo in caso di necessità.

Art. 4

Principi generali e garanzie

Le prescrizioni del presente regolamento si fondano sui principi di liceità, necessità, proporzionalità e finalità.

Principio di liceità: il trattamento dei dati personali da parte dei soggetti pubblici è consentito soltanto per lo svolgimento di funzioni istituzionali, in base alla normativa vigente.

Principio di necessità: il sistema di videosorveglianza è configurato per l'utilizzazione al minimo di dati personali ed identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi od opportune modalità, che permettano di identificare l'interessato solo in caso di necessità.

Principio di proporzionalità: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività non soggette a concreti pericoli, o per le quali non ricorra una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili.

Principio di finalità: gli scopi perseguiti devono essere determinati, espliciti e legittimi.

Art. 5

Finalità dell'impianto

L'attività di videosorveglianza, essendo relativa allo svolgimento di funzioni istituzionali, non ha ad oggetto il trattamento dei dati sensibili, non potendosi tuttavia escludere che le registrazioni effettuate siano idonee a far risalire a tali informazioni. L'uso di impianti di videosorveglianza cittadina è uno strumento adoperato per l'attuazione di un sistema integrato di politiche per la sicurezza urbana così come previsto dal D.L. n. 11/2009 convertito con L. n. 38/2009.

In particolare, gli impianti assolvono alle seguenti finalità:

- Monitorare la regolare circolazione lungo le strade comunali;
- Riprendere le immagini di specifici siti comunali;
- Tutelare il patrimonio comunale;
- Controllare determinate aree ai fini preventivi di danneggiamenti, atti di vandalismo, condotte illecite ed episodi di microcriminalità;
- Funzioni di Protezione Civile.

La disponibilità tempestiva di immagini e dati presso la Centrale di Controllo costituisce uno strumento di prevenzione e razionalizzazione dell'azione della Polizia Municipale, in particolare nell'ambito del monitoraggio del traffico e di controllo del territorio nelle vie del centro abitato.

Il Comune promuove ed attua, per la parte di competenza, politiche di controllo del territorio, integrate con organi istituzionalmente preposti alla sicurezza pubblica. A tal fine, previa intesa o su richiesta delle autorità di pubblica sicurezza e degli organi di polizia, può disporre l'utilizzo degli impianti comunali di videosorveglianza ai fini di prevenzione e repressione di atti delittuosi. I dati così raccolti vengono utilizzati esclusivamente dalle autorità ed organi anzidetti.

Art. 6

Caratteristiche tecniche e Responsabile dell'impianto

Il sistema di videosorveglianza sarà costituito da telecamere fisse e/o mobili destinate al controllo delle vie e degli spazi pubblici del Comune di Campo nell'Elba, tutte attive 24 ore e da un centro di gestione che registra, conserva e cancella dopo il tempo previsto le immagini registrate. Il centro di gestione avrà sede presso la Centrale di Controllo della Polizia Municipale, presso cui saranno presenti apparecchiature di registrazione ed archiviazione delle immagini.

Il sistema di videosorveglianza sarà a circuito chiuso e trasmetterà le immagini mediante la rete dedicata e protetta; le immagini saranno inaccessibili da qualunque apparecchiatura in rete non abilitata all'accesso, pertanto, è esclusa l'interconnessione con altri sistemi oltre a quello di visualizzazione delle centrali operative, o con archivi dati, nonché l'accesso ad altri terminali ed elaboratori.

Le immagini verranno registrate su un server dati INVR accessibile solamente al personale autorizzato per la gestione e manutenzione del sistema, attraverso l'uso delle proprie credenziali. Il sistema consentirà di volta in volta all'operatore autorizzato la visione in tempo reale delle immagini e, limitatamente al responsabile dell'impianto, l'accesso alle immagini videoregistrate, conservate sotto forma di dati digitali, attraverso programma riservato e l'eventuale trasferimento dei dati d'archivio su analogo supporto.

La rete di comunicazione sarà basata principalmente su dorsali in fibra ottica multimodale 50/125, che costituisce la maggior parte del sistema di comunicazione destinato al sistema TVCC. I nodi di rete, realizzati in appositi armadi stradali, consentiranno di alloggiare gli apparati transceiver che permetteranno di collegare sia le telecamere Ip raggiunte tramite cavo LAN, sia le telecamere analogiche collegate mediante l'utilizzo di cavo RG11 in rame. All'interno degli armadi stradali saranno alloggiati anche i dispositivi di alimentazione e protezione elettrica adibiti ad alimentare le apparecchiature in campo.

La rete di comunicazione disporrà di un accesso alla rete internet che permetterà:

- 1) L'accesso a potenziali client remoti, quali alte FF.OO, per le quali sarà possibile creare degli appositi profili di accesso al server Recorder INVR.
- 2) La connessione diretta, per le pattuglie in servizio, a tutte le telecamere, in special modo alle TECNOSENSE PVZoom HD Dual-E OS.

Ogni modifica concernente le caratteristiche tecniche dell'impianto di videosorveglianza potrà esser fatta mediante apposita Determina Dirigenziale, a seguito di Delibera di Giunta Comunale.

Art. 7

Uso delle telecamere

Il sistema di videosorveglianza prevede una ripresa dei luoghi che non rileva percorsi o caratteristiche fisionomiche, come ad esempio il riconoscimento facciale, eventi improvvisi, oppure comportamenti non previamente classificati. E 'previsto l'uso della mobilità della telecamera solo nei seguenti casi:

- a) Per il controllo e la registrazione di atti illeciti perpetrati all'interno del campo iniziale di registrazione della telecamera e che rischierebbe di sfuggire al controllo per lo spostamento dei soggetti interessati;
- b) In caso di comunicazione, anche verbale e telefonica, di situazioni di illecito o di pericolo segnalate al responsabile dell'impianto, da verificarsi immediatamente;
- c) Nel supporto logistico ad operazioni di polizia condotte con personale sul luogo

Le inquadrature saranno tali da cogliere un'immagine panoramica delle persone e dei luoghi, evitando riprese inutilmente particolareggiate tali da essere eccessivamente intrusive della riservatezza delle persone, garantendo comunque la possibilità di identificazione per esigenze inerenti la sicurezza pubblica o l'accertamento, la prevenzione e repressione di reati e violazioni amministrative, quando il pericolo è concreto e specifico di lesione di un bene.

Art. 8 **Informativa**

La presenza di un impianto di videosorveglianza deve essere resa pubblica, a cura del responsabile dell'impianto, attraverso i mezzi che si riterranno più idonei, ed in particolare:

- a) L'affissione del presente regolamento e del nominativo del "Responsabile dell'impianto", di cui all'art. 6 del presente Regolamento, in modo stabile all'Albo Pretorio ed in forma cartacea presso il Comando di Polizia Municipale;
- b) Un certo numero di cartelli verranno posizionati nelle zone ove è presente la videosorveglianza, collocandoli in luoghi ripresi o nelle immediate vicinanze ma non necessariamente a contatto con le telecamere. In presenza di più telecamere, in relazione alla vastità dell'area ed alle modalità delle riprese, andranno installati più cartelli.

Gli interessati dovranno essere informati che stanno per accedere o che si trovano in una zona videosorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa "minima" in ottemperanza a quanto richiesto ex art. 13 D.lgs 196/03 e s.m., con particolare riguardo alle finalità ed all'eventuale conservazione.

Il Comune di Campo nell'Elba si obbliga, pertanto, ad affiggere nelle strade, parchi o piazze interessate un'adeguata segnaletica su cui verrà riportata la seguente dicitura:

"Comune di Campo nell'Elba – Area videosorvegliata. La registrazione è effettuata dal Comune per fini di sicurezza urbana (ex art. 13 D.Lgs 196/03 e s.m.)".

Il Responsabile del trattamento rende nota l'attivazione dei sistemi di videosorveglianza ed il conseguente avvio del trattamento dei dati personali, l'eventuale incremento dimensionale degli impianti e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo. Con un preavviso di 10 giorni, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale. L'uso dei dati personali non necessita di consenso da parte degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate dalla legge sulla privacy ad un regime di tipo particolare.

Art. 9 **Trattamento dei dati personali per finalità istituzionali**

Il trattamento dei dati personali è effettuato, a seguito di attivazione di un impianto di videosorveglianza, sul territorio comunale di Campo nell'Elba nel rispetto delle finalità istituzionali e dei principi normativi. Le finalità istituzionali del suddetto impianto sono conformi alle funzioni demandate al Comune di Campo nell'Elba, anche con riferimento al più ampio concetto di "sicurezza urbana", richiamata dal D.L. 11/2009 (decreto sicurezza) e dalla Legge di conversione n. 38/09 ed

esplicata ulteriormente dal D.M. del Ministero dell'Interno del 05/08/2008 e dalla susseguente elaborazione giurisprudenziale (Corte Cost. sentenza n. 196/2009) che la definisce come la "prevenzione dei reati e la tutela dei primari interessi pubblici sui quali si regge l'ordinata e civile convivenza nella comunità nazionale".

Le finalità istituzionali vengono pertanto classificate in:

- a) Prevenire e reprimere atti delittuosi;
- b) Tutelare gli immobili facenti parte del patrimonio pubblico;
- c) Tutela dell'incolumità pubblica dei cittadini con particolare attenzione alle fasce più deboli;
- d) Controllo di determinate aree abusivamente impiegate come discariche di materiali;
- e) Monitoraggio del rispetto delle disposizioni comunali in materia di abbandono di rifiuti;
- f) Segnalazione contestuale di alcune tipologie di infrazioni al C.d.S. che potranno essere oggetto di contestazione immediata dal personale con qualifica di polizia stradale;
- g) Monitoraggio e controllo del traffico in tempo reale;
- h) Acquisire fonti di prova a seguito di commissione di reati;
- i) Funzioni di Protezione Civile.

Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 della L. 300/70 (Statuto dei lavoratori) 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, inoltre, essere utilizzati per finalità statistiche o per la finalità di promozione turistica. I dati raccolti per i fini di cui al presente regolamento, non potranno essere utilizzati per finalità diverse o ulteriori e, salvo esigenze di polizia o giustizia, non dovranno essere diffusi o comunicati a terzi.

Art. 10

Titolare e Responsabile del trattamento

Il Sindaco in qualità di rappresentante del Comune è Titolare del trattamento di dati personali e designa mediante Decreto il Responsabile del trattamento, che viene individuato nella figura del Comandante di Polizia Municipale, disciplinandone la materia trattata, la durata, la natura, le finalità, gli obblighi ed i diritti dell'incarico.

E' consentita la nomina, tramite atto scritto, di incaricati del trattamento da parte del Responsabile per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il titolare ed il responsabile. Le operazioni di trattamento potranno essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile, attenendosi alle istruzioni da lui impartite per iscritto.

Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato degli stessi. Il Responsabile del trattamento garantisce che, chiunque agisca sotto la sua autorità ed abbia accesso a dati personali, sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

Il Responsabile del trattamento adotta idonee misure tecniche e organizzative, adeguate per garantire la sicurezza dei trattamenti, in particolare custodisce le chiavi di accesso ai locali della sala di controllo e degli armadi per la conservazione delle registrazioni e dei verbali di accertamento, nonché le parole chiave per l'utilizzo dei sistemi.

Art. 11 Notificazione

I dati trattati dovranno essere notificati al Garante per la protezione dei dati personali nei casi specificatamente previsti dalla normativa vigente sulla privacy. A tale proposito le disposizioni vigenti prevedono che non vadano comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini conservate temporaneamente per esclusiva finalità di sicurezza o di tutela delle persone e del patrimonio. Il Titolare del trattamento provvede a richiedere la verifica preliminare prima di mettere in funzione le telecamere nei casi previsti dalle disposizioni impartite dal Provvedimento del Garante Privacy in materia di videosorveglianza dell'8 aprile 2010.

Art. 12 Responsabile della protezione dati (RPD)

Il Responsabile protezione dati (in seguito indicato con l'acronimo RPD) potrà essere individuato tra i dipendenti di ruolo del Comune purché in possesso di idonee capacità professionali e che non si trovi in situazione di conflitto d'interesse, ovvero in alternativa, nella figura d'impresa e/o professionista scelto tramite procedura ad evidenza pubblica. Il RPD è incaricato dei seguenti compiti:

- a) Informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa relativa alla protezione dei dati;
- b) Sorvegliare l'osservanza della normativa relativa alla protezione dei dati, nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- c) Fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- d) Cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento;
- e) Conservare o delegare la conservazione dei registri delle attività di trattamento e delle categorie di attività trattate;
- f) Assicurare altri compiti e funzioni in materia che non costituiscano conflitto d'interesse.

Il RPD è invitato a partecipare alle riunioni di coordinamento che abbiano oggetto questioni inerenti la protezione dei dati personali, deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da rendere una consulenza idonea, scritta od orale.

Il parere del RPD è obbligatorio e non vincolante ma, nel caso la decisione assunta sia difforme da quella raccomandata, sarà necessario motivare specificatamente tale scelta. L'RPD deve essere informato tempestivamente qualora si verifichi una violazione dei dati o altro incidente tecnico.

La figura del RPD è incompatibile con chi determina le finalità od i mezzi del trattamento, in particolare con: il Responsabile per la prevenzione della corruzione e trasparenza, il Responsabile del trattamento e con qualsiasi altro incaricato che compori la determinazione di finalità o mezzi del trattamento.

Art. 13

Nomina degli incaricati alla gestione dell'impianto di videosorveglianza

Il Responsabile del trattamento designa e nomina gli incaricati del trattamento in numero sufficiente a garantire la gestione del servizio di video sorveglianza tra il personale che, per esperienza, capacità, affidabilità, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati. Con l'atto di nomina verranno designati i soggetti cui è affidata la custodia e la conservazione delle password e delle chiavi di accesso alla sala di controllo ed agli armadi per la conservazione dei supporti. Ai singoli preposti saranno affidati compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti sul corretto uso dei sistemi, sulla normativa di riferimento e sul presente regolamento. La gestione dell'impianto di videosorveglianza è riservata agli organi di Polizia Municipale ed i dati personali oggetto del trattamento saranno custoditi presso la Centrale di Controllo, dove è installata la postazione di registrazione, a cui può accedere solo ed esclusivamente il personale in servizio della Polizia Municipale, debitamente istruito, incaricato ed autorizzato.

Art. 14

Accertamento di illeciti e indagini di autorità giudiziaria e forze di polizia

Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale l'incaricato della videosorveglianza provvederà a darne immediata comunicazione agli organi competenti. In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa di cui al precedente art. 7, l'incaricato procederà agli ingrandimenti della ripresa delle immagini strettamente necessarie e non eccedenti allo specifico scopo perseguito ed alla registrazione delle stesse su supporti magnetici.

Alle informazioni raccolte ai sensi del presente articolo potranno accedere, a seguito di richiesta scritta, solo gli organi di Polizia Giudiziaria e l'Autorità Giudiziaria per le indagini necessarie.

Gli apparati potranno essere utilizzati anche in relazione ad apposite e specifiche indagini di Autorità Giudiziaria o di organi di Polizia.

Art. 15

Misure di sicurezza e limiti di utilizzo

Le aree in cui verranno installate le telecamere sono localizzate all'interno del relativo capitolato tecnico del Comune e potranno essere identificate mediante delibera di Giunta comunale che ne motiverà la scelta. L'accesso ai sistemi è esclusivamente consentito al Responsabile ed ai preposti come indicato agli articoli precedenti. L'accesso alle immagini registrate dovrà essere effettuato esclusivamente in caso di eventi criminosi o di danni al patrimonio comunale. In nessun caso i dati trattati dovranno esser diffusi o comunicati a terzi, salvo che si tratti indagini giudiziarie o di polizia da comunicare alla competente A.G.

Dovranno essere previsti diversi livelli di accesso al sistema e di utilizzo delle informazioni, attraverso una doppia chiave, fisica e logica che consenta una immediata ed integrale visione delle immagini solo in caso di necessità. Le chiavi di accesso fisico alla sala di controllo saranno distribuite in copia dal Responsabile del trattamento agli incaricati che la dovranno custodire diligentemente impedendone l'uso a persone non autorizzate.

Gli incaricati e, su richiesta, le altre forze di polizia saranno dotati di una propria password di accesso al sistema che dovrà esser mantenuta segreta e potrà essere autonomamente variata con comunicazione scritta al Responsabile del trattamento. Il sistema dovrà essere fornito di "log" di accesso, che saranno conservati per la durata di un anno. Il presidio della centrale di controllo non è garantito 24 ore ma in base alla concreta organizzazione del servizio del Comando di Polizia Municipal

Art. 16

Trattamento e conservazione dei dati

Le operazioni di trattamento verranno riportate in appositi verbali di accertamento in cui vengono descritte le operazioni eseguite dagli autorizzati e le eventuali registrazioni saranno custodite in copia, mediante supporti magnetici od ottici, all'interno degli armadi della centrale di controllo. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai 7 giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione, ai sensi dell'art. 6 c. 8° della L. n. 38/2009. In tutti i casi in cui si voglia procedere ad un allungamento dei tempi di conservazione per un periodo superiore a quello indicato precedentemente, andrà inoltrata specifica richiesta al Garante per la necessaria verifica preliminare, ipotizzando la fattispecie come eccezionale nel rispetto del principio di proporzionalità, con riferimento alle esigenze di sicurezza perseguite, alle concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia all'Autorità Giudiziaria o alla Polizia Giudiziaria in relazione ad una attività investigativa in corso.

Art. 17

Modalità di raccolta dei dati

Le telecamere del sistema di videosorveglianza consentiranno riprese video a colori o in bianco e nero, comprese quelle in visione notturna, potranno essere dotate di brandeggio zoom ottico programmato e sono collegate alla LAN comunale (o in VLAN separata) che potrà, esclusivamente per il perseguimento dei fini istituzionali, eventualmente digitalizzare o indicizzare le immagini. I segnali video delle unità di ripresa saranno raccolti presso apposito apparato dedicato ubicato nei locali del CED comunale c/o sala operativa della Polizia Municipale o altra sala idonea. La raccolta dei dati, nel caso in cui l'Amministrazione lo valuti maggiormente efficiente, economico e sicuro, potrà alternativamente essere affidata ad un soggetto esterno appositamente incaricato tramite apposito atto che individuerà la persona preposta, la quale dovrà comunque attenersi a tutto quanto previsto dal presente regolamento. Le immagini videoregistrate saranno conservate per il periodo indicato nell'art. 16, dopodiché saranno cancellate in automatico dal sistema mediante sovra-registrazione, in modalità tale da rendere non più utilizzabili i dati cancellati.

Art. 18

Obblighi degli operatori

L'utilizzo del brandeggio da parte degli operatori incaricati del trattamento dovrà essere conforme ai limiti indicati nel presente regolamento. La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

In particolare, i compiti affidati agli incaricati sono quelli di:

- a) Trattare tutti i dati personali di cui vengono a conoscenza nell'ambito dello svolgimento delle funzioni in modo lecito e secondo correttezza;
- b) Accedere ai dati unicamente con le credenziali assegnate senza che queste vengano comunicate a soggetti terzi non autorizzati;
- c) Effettuare la sola consultazione esclusivamente per lo svolgimento delle proprie mansioni;

- d) Verificare che le registrazioni non superino i termini temporali di legge, ovvero 7 giorni salvo eccezioni precedentemente indicate, controllando che la sovra-registrazione sia attiva;
- e) Comunicare al Responsabile e/o al Titolare eventuali richieste di accesso ex art. 7 D.lgs 196/03 e s.m.;
- f) Comunicare al Responsabile e/o al Titolare eventuali accessi non autorizzati da parte di soggetti terzi negli ambienti in cui risiedono gli schermi e le registrazioni;
- g) Non creare salvataggi dati o banche dati derivanti dalla raccolta effettuata per il tramite degli impianti di videosorveglianza, senza espressa autorizzazione scritta del responsabile;
- h) Mantenere assoluto riserbo sui dati personali di cui vengono a conoscenza nell'esercizio delle loro funzioni;
- i) Prendere visione del presente regolamento, il quale costituisce a tutti gli effetti documento formativo-informativo per un corretto uso della strumentazione necessaria al funzionamento dell'impianto;
- j) Partecipare al necessario corso formativo finalizzato al corretto uso del sistema degli impianti.

Art. 19

Registro unico delle attività di trattamento

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

- a) Il nome ed i dati di contatto del Comune, del Sindaco o del suo delegato, del RPD;
- b) Le finalità del trattamento;
- c) La sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- d) Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- e) Ove stabilito, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- f) Il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate;

Il registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato presso gli uffici della struttura organizzativa del Comune, in forma telematica/cartacea. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il registro, sotto la responsabilità del medesimo Titolare. Il Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro. Il Titolare può decidere di tenere un Registro unico dei trattamenti o un Registro delle categorie trattate con i relativi Registri di trattamento.

Art. 20

Valutazioni d'impatto sulla protezione dei dati

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare prima di effettuare il trattamento deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGPD, considerati la natura, l'oggetto, il contesto e la finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35 RGPD. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35 RGPD, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

- a) Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

- b) Le decisioni automatizzate che producono significativi effetti giuridici o di analogia natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
- c) Monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
- d) Trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 RGPD;
- e) Trattamenti di dati su larga scala, tenendo conto del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
- f) Combinazione o raffronto di insiemi di dati, secondo le modalità che esulano dalle ragionevoli aspettative dell'interessato;
- g) Dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
- h) Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- i) Tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopraindicati occorrerà, in via generale, condurre una DPIA salvo che il Titolare ritenga motivatamente che la stessa non può presentare un rischio elevato. Il Titolare potrà altresì motivatamente ritenere che per un trattamento che soddisfi solo uno dei criteri di cui sopra, occorra comunque la conduzione di una DPIA. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa, con la possibilità di affidare la conduzione materiale della stessa ad un altro soggetto, interno o esterno al Comune.

Il Titolare dovrà consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA e tale consultazione e le decisioni assunte dovranno essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA ed il Responsabile del trattamento dovrà assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il Responsabile della sicurezza dei sistemi informativi, se nominato e/o l'ufficio competente per detti sistemi, forniranno supporto al Titolare per lo svolgimento della DPIA. Il RPD potrà proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Il Responsabile della sicurezza dei sistemi informativi, se nominato e/o l'ufficio competente per detti sistemi, potranno proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

La DPIA non sarà necessaria nei seguenti casi:

- a) Se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35 RGPD;
- b) Se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- c) Se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RPD e che proseguono con le stesse modalità oggetto di tale verifica.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

- 1) Descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati;
- 2) Valutazione della necessità e proporzionalità dei trattamenti;
- 3) Valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, le particolarità e le gravità dei rischi di ogni singolo rischio;
- 4) Individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare potrà raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione sarà specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati. Il Titolare dovrà consultare il Garante Privacy prima di procedere al trattamento, se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima Autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

La DPIA dovrà essere effettuata con eventuale riesame delle valutazioni condotte anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 21

Cessazione del trattamento dei dati

In caso di cessazione per qualsiasi causa di un trattamento, i dati personali saranno distrutti o conservati per fini esclusivamente istituzionali dell'impianto attivato.

Art. 22

Diritti dell'interessato nel trattamento dei dati

In relazione al trattamento dei dati personali dovrà essere assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti in conformità al Codice Privacy, in particolare quello di accedere ai dati che lo riguardano, di verificarne le finalità, le modalità del trattamento e di ottenerne l'interruzione nel caso di utilizzo illecito, in particolare per la carenza dell'adozione delle idonee misure di sicurezza o per l'uso indebito da parte di soggetti non autorizzati.

L'interessato, dietro presentazione di apposita istanza avrà diritto:

- a) Ad essere informato sugli estremi identificativi del Titolare e del Responsabile, oltre che delle finalità e le modalità del trattamento dei dati;
- b) Di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;
- c) Di opporsi, in tutto o in parte e per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- d) Ad ottenere, a cura del responsabile e senza ritardo e comunque non oltre 15 giorni dalla data di ricezione della richiesta:
 - La conferma dell'esistenza o meno di dati personali che lo riguardano
 - La trasmissione in forma intelligibile dei medesimi dati e della loro origine
 - L'informazione sulle procedure adottate in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento, la cancellazione, 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.

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 sopracitati l'interessato può conferire, per iscritto, per delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato potrà altresì farsi assistere da persona di fiducia.

Le istanze di cui al presente articolo potranno essere trasmesse mediante lettera raccomandata, telefax, posta elettronica o posta elettronica certificata al Titolare o al Responsabile del trattamento, i quali dovranno provvedere in merito e non oltre 15 giorni. L'istanza dovrà indicare a quale impianto di sorveglianza si fa riferimento, il giorno e l'ora in cui il richiedente potrebbe essere stato oggetto di ripresa. Qualora tali indicazioni manchino o siano insufficienti a permettere il reperimento delle immagini, di ciò deve essere data comunicazione al richiedente, così come nell'ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione. Il Responsabile del trattamento è tenuto ad accertare l'effettiva esistenza delle immagini dandone comunicazione al richiedente; nel caso di accertamento positivo fissa il giorno, l'ora ed il luogo in cui l'interessato potrà visionare le immagini che lo riguardano

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

La risposta ad una richiesta di accesso a dati conservati dovrà riguardare tutti quelli attinenti al richiedente identificabile e potrà comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice della Privacy, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato. In riferimento alle immagini registrate non sarà in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo; viceversa l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.

Art. 23

Danni cagionati per effetto del trattamento di dati personali

Ai sensi dell'art. 82 RGPD, chiunque subisca un danno materiale o immateriale causato da una violazione della normativa in questione avrà diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento. Il Titolare del trattamento risponde per il danno cagionato dal trattamento che violi il presente regolamento. Il Responsabile del trattamento risponde per il danno causato solo se non ha adempiuto gli obblighi specifici e diretti agli incaricati o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. Il Titolare o il Responsabile sono esonerati dalla responsabilità se dimostrano che l'evento dannoso non gli è in alcun modo imputabile.

Qualora più figure siano coinvolte nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni soggetto sarà responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato. Qualora uno dei soggetti abbia pagato l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento, avrà diritto di reclamare agli altri soggetti titolari o responsabili coinvolti la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno causato.

Art. 24

Tutela amministrativa e giurisdizionale

Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto nella parte terza del D.Lgs 196/03 e s.m.

In sede amministrativa il Responsabile del trattamento dei dati personali, ai sensi degli artt. 4-6 della L. n. 241/90, è anche il Responsabile del procedimento amministrativo.

Art. 25

Provvedimenti attuativi

Compete alla Giunta Comunale l'assunzione dei provvedimenti attuativi, nonché la definizione di ogni ulteriore e specifica disposizione ritenuta utile, in coerenza con gli indirizzi stabiliti dal presente Regolamento.

Art. 26

Norma di rinvio

Per tutto quanto non espressamente disciplinato con il presente Regolamento, si applicano le disposizioni del Codice della Privacy e del RGPD, comprensive di tutte le sue norme attuative vigenti e le linee guida del Garante per la protezione dei dati personali.

Il contenuto dello stesso dovrà essere aggiornato nei casi di variazione della normativa in materia di trattamento dei dati personali.

Copia del presente regolamento dovrà essere tenuto a disposizione del Garante per la protezione dei dati personali, presso il Comando di Polizia Municipale di Campo nell'Elba.

Art. 27

Entrata in vigore

Il presente Regolamento, dopo l'esecutività della deliberazione del Consiglio Comunale che lo approva, è pubblicato per 15 giorni all'Albo pretorio ed entra in vigore il giorno successivo all'ultimo di pubblicazione.

MODELLO 1
PER RICHIESTA DI ACCESSO ALLA CENTRALE DI CONTROLLO PER LA
VISUALIZZAZIONE DI IMMAGINI IN DIRETTA

N...../Reg.....

Il sottoscritto.....
identificato tramite.....
in servizio presso.....
per motivi di.....
chiede di accedere alla sala di controllo per visualizzare le immagini in diretta della telecamera n...
ubicata in via.....

Marina di Campo lì,.....

I Richiedenti

.....
.....
.....

MODELLO 2
PER RICHIESTA DI ACCESSO ALLA CENTRALE DI CONTROLLO PER LA
VISUALIZZAZIONE DI IMMAGINI VIDEOREGISTRATE

N...../Reg.....

Il sottoscritto.....
identificato tramite.....
in servizio presso.....
per motivi di.....
chiede di accedere alla sala di controllo per visualizzare le immagini videoregistrate della telecamera
n.....ubicata in via.....

Marina di Campo lì,.....

I Richiedenti

.....
.....
.....

MODELLO 3
PER RICHIESTA DI ACCESSO ALLA CENTRALE DI CONTROLLO PER IL
SALVATAGGIO E/O L'ESTRAPOLAZIONE DELLE IMMAGINI VIDEOREGISTRATE

N...../Reg.....

Il sottoscritto.....
identificato tramite.....
in servizio presso.....
per motivi di.....
chiede di accedere alla sala di controllo per visualizzare, salvare ed estrapolare le immagini
videoregistrate della telecamera n..... ubicata in via.....

Marina di Campo lì,.....

I Richiedenti

.....
.....
.....

MODELLO 4
PER RICHIESTA DI ACCESSO ALLA CENTRALE DI CONTROLLO PER LA
MANUTENZIONE DELLE APPARECCHIATURE DI VIDEOSORVEGLIANZA

N...../Reg.....

Il sottoscritto.....
identificato tramite.....
in servizio presso.....
per motivi di.....
chiede di accedere alla sala di controllo per visualizzare le immagini videoregistrate della telecamera
n..... ubicata in via.....

Marina di Campo lì,.....

I Richiedenti

.....
.....
.....