Ente di Gestione per
i Parchi e la Biodiversità
Emilia Orientale

Regolamento generale in materia di videosorveglianza

.....

Approvato con Delibera n. 79 del 19/12/2024

Sommario

CAPO I – DISPOSIZIONI GENERALI PRINCIPI

Sezione I – Oggetto, riferimenti e definizioni

1. Oggetto del regolamento

1.1 Il presente regolamento disciplina il trattamento dei dati personali acquisiti mediante l'utilizzo di sistemi di videosorveglianza, compresi i trattamenti di dati personali a mezzo di nuove tecnologie, effettuati dall'Ente titolare.

2. Riferimenti normativi

2.1 Il presente regolamento è stato redatto tenendo conto del seguente quadro normativo:

- Legge 7 marzo 1986, n. 65;
- Art. 54 del D. Lgs. 18 agosto 2000 n. 267 e successive modificazioni;
- D.L. 23 febbraio 2009 n. 11, coordinato con Legge di conversione n. 38 del 23 aprile 2009 recante: "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori", ed in particolare dall'art. 6;
- Circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/N471;
- Decreto del Ministero dell'interno datato 5 agosto 2008;
- "Provvedimento in materia di videosorveglianza" emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010;
- Circolare n. 558/SICPART/422.2/47/316370 datato 8 giugno 2017 del Capo della Polizia, recante: "Patti per l'attuazione della sicurezza urbana – Forza di Intervento Rapido";
- Decreto del Presidente della Repubblica 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";

- Regolamento UE n. 2016/679 – Regolamento generale sulla protezione dei dati personali (di seguito anche 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";
- D.Lgs. 30 giugno 2003 n. 196: "Codice in materia di protezione dei dati personali", come modificato e riformato dal D.lgs. n. 101/2018 recante le "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- D.Lgs. del 18 maggio 2018, n, 51, recante: "Attuazione della direttiva (UE) 2016/680 del Parlamento e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2018/977 GAI del Consiglio".

Sezione II – Principi generali

3. I principi di finalità e liceità

3.1 I trattamenti di dati personali effettuati dall'Ente Titolare a mezzo dei sistemi di videosorveglianza sono effettuati a norma dell'articolo 6, paragrafo 1, lettera e) del GDPR poiché il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e, per gli aspetti più attinenti alla prevenzione a fini di indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, i trattamenti sono effettuati in aderenza al D.lgs. n. 51/2018.

3.2 Per ciascuna delle finalità di trattamento disciplinate nel presente regolamento l'Ente Titolare conduce, ai sensi dell'art. 35 del GDPR, valutazione d'impatto.

4. Principio di correttezza e trasparenza

4.1 L'Ente Titolare effettua il trattamento di dati a mezzo dei sistemi di videosorveglianza secondo il principio di correttezza, ovvero i dati personali non sono trattati in modo pregiudizievole, discriminatorio, imprevisto o fuorviante per l'interessato.

4.2 In correlazione al principio di cui al comma che precede, l'Ente Titolare effettua il trattamento di dati in maniera trasparente nei confronti degli interessati, installando cartelli visibili, fornendo informazioni chiare e puntuali sulle modalità di trattamento e rappresentando come i cittadini possono interloquire con l'Amministrazione in ordine all'esercizio dei diritti di cui agli artt. 15-22 del GDPR.

5. Principio di necessità

5.1 L'Ente Titolare ha valutato che non è possibile perseguire le finalità di cui al presente regolamento con misure alternative alla videosorveglianza, poiché inefficaci.

5.2 I sistemi di videosorveglianza sono installati, configurati e programmati in modo da escludere ogni uso superfluo o ridondante di immagini e dati personali.

6. Principio di proporzionalità e minimizzazione dei dati

6.1 Il trattamento di dati personali tramite un sistema di videosorveglianza è lecito solo se è rispettato il principio di proporzionalità (cfr. articolo 5, lettera b) GDPR) e i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, in aderenza all'articolo 5, paragrafo 1, lettera c) del GDPR.

6.2 Le modalità di effettuazione del trattamento di dati tramite sistemi di videosorveglianza, tra cui il numero di videocamere, le modalità di ripresa e la dislocazione delle stesse, e l'accesso alle immagini sono definite in aderenza agli scopi prefissati.

7. Principio di limitazione della conservazione

7.1 L'Ente Titolare definisce specifici tempi di cancellazione in relazione alle finalità e ai sistemi di videosorveglianza utilizzati.

7.2 L'Ente Titolare implementa sistemi che cancellano le registrazioni dopo un periodo di tempo predefinito, fatta eccezione per i casi espressamente previsti dalla legge e dal presente regolamento.

8. Principio di integrità e riservatezza

8.1 L'Ente Titolare protegge adeguatamente i dati personali contro l'accesso, la divulgazione, l'alterazione e la distruzione non

autorizzati, mantenendo in sicurezza mediante misure tecniche e organizzative appropriate.

8.2 L'Ente Titolare può implementare, tramite apposito disciplinare tecnico, soluzioni di:

- crittografia per proteggere i flussi video e le registrazioni archiviate, sia che si trovino su server locali che in cloud;
- controllo degli accessi, limitando l'accesso alle registrazioni video solo al personale autorizzato;
- autenticazione nominativa e con password policy robuste;
- registrazioni di log per monitoraggio del buon funzionamento e verifiche di sicurezza informatica;
- profilazione che consenta di assegnare agli interessati diversi livelli di visibilità e trattamento delle immagini in aderenza alle differenti e specifiche competenze attribuite ai singoli operatori;
- protezione delle infrastrutture di rete e dei server, garantendo che queste siano protette da attacchi esterni, come l'hacking o il software malevolo;
- formazione del personale autorizzato, anche in ordine alla protezione dei dati personali e alla sicurezza informatica.

CAPO II – Responsabilità del trattamento

9. Titolare del trattamento e responsabilità connesse al trattamento

9.1 Il Titolare del trattamento dei dati è l'**Ente di gestione per i Parchi e la biodiversità-Emilia orientale**, che ha aggiornato compiti e responsabilità in ordine agli adempimenti in materia di protezione dei dati personali con la delibera 67 del 14/11/2024.

9.2 In aderenza alla deliberazione di cui al comma precedente, il Titolare del trattamento nomina i Soggetti attuatori o Designati al trattamento, secondo il modello organizzativo adottato,

ovvero i soggetti in capo ai quali in relazione alle specifiche finalità previste è attribuita la responsabilità dei trattamenti di dati personali effettuati a mezzo dei sistemi di videosorveglianza.

9.3 In capo al soggetto di cui al comma 9.1 sussiste l'onere, ai sensi e per gli effetti di cui all'art. 28 del GDPR, di nominare responsabili del trattamento i soggetti fornitori dei servizi correlati alla videosorveglianza.

9.4 Per gli aspetti tecnologici, ivi comprese le adeguate misure di sicurezza, i Soggetti attuatori o Designati al trattamento, secondo il modello organizzativo adottato, vanno nominati nell'ambito dello specifico ruolo svolto per ciascun trattamento effettuato tramite sistemi di videosorveglianza.

9.5 In capo al soggetto di cui al comma 9.1 sussiste l'onere di condurre, ai sensi dell'art. 35 del GDPR, apposita valutazione di impatto per ciascuna delle diverse finalità di trattamento riportate nel presente regolamento.

10. Soggetti autorizzati

10.1 Il trattamento di dati personali mediante l'impiego di sistemi di videosorveglianza è consentito esclusivamente ai soggetti preventivamente autorizzati.

10.2 L'autorizzazione al trattamento dei dati personali dei soggetti incaricati deve avvenire per iscritto e deve essere circoscritta ad un numero limitato di persone.

10.3 Ai soggetti autorizzati è somministrata adeguata formazione in ordine alla normativa in materia di protezione dei dati personali e alle funzionalità del sistema di videosorveglianza utilizzato.

CAPO III - Videosorveglianza per finalità di sicurezza urbana

11. I trattamenti di dati personali effettuati per finalità di sicurezza urbana

11.1 L'Ente Titolare effettua trattamenti di dati personali a mezzo dei sistemi di videosorveglianza, ai sensi dell'art. 4 del Decreto-Legge n. 14/2017 convertito con modificazioni dalla L. 18 aprile 2017, n. 48 per finalità di sicurezza urbana.

11.2 L'Ente Titolare pianifica le realizzazioni degli impianti di videosorveglianza cittadina volti alle finalità di cui al presente articolo, in un quadro di integrazione e sinergia con gli Enti del territorio, condividendo con il Comitato Provinciale per l'Ordine e la Sicurezza Pubblica i progetti di installazione di sistemi di videosorveglianza, anche al fine di evitare una ingiustificata proliferazione di tali apparati, oltre che per assicurare la necessaria interoperabilità tra i sistemi dei diversi attori del territorio coinvolti.

11.3 Il sistema di videosorveglianza è costituito dall'insieme degli apparati elencati nel documento allegato al presente regolamento e pubblicato sul sito istituzionale dell'Ente Titolare del trattamento che descrive anche la posizione delle telecamere sul territorio cittadino. Il Soggetto attuatore o Designato al trattamento secondo il modello organizzativo adottato di cui al punto 9.2 del presente regolamento provvede al suo aggiornamento riportando le modifiche e le integrazioni direttamente nel documento pubblicato.

12. Accesso alle immagini

12.1 La visualizzazione in diretta delle immagini e l'accesso ai dati conservati per la duplicazione e la loro differita visualizzazione è strutturata secondo distinti livelli di profilazione stabiliti con apposito atto dal Soggetto attuatore o Designato al

trattamento, secondo il modello organizzativo adottato, eventualmente corredato da un Disciplinare ad uso interno contenente istruzioni tecniche più dettagliate agli operatori autorizzati.

12.2 La consultazione dei dati può essere effettuata:

- per esigenze di manutenzione degli impianti;
- in caso di richiesta di accesso dell'interessato ai propri dati personali, nonchè ai sensi dell'art. 24 della L. n. 241/1990;
- nell'esercizio delle finalità di cui all'articolo precedente dai soggetti precipuamente autorizzati;
- al fine di assolvere agli oneri derivanti da richieste dell'Autorità Giudiziaria;
- nel caso di visite ispettive da parte dell'Autorità Garante per la protezione dei dati personali.

13. Tempi di conservazione delle immagini

13.1 Le immagini registrate mediante il sistema di videosorveglianza per le finalità di cui all'art. 11 sono conservate per massimo di sette giorni. Decorso tale periodo, i dati registrati sono cancellati con modalità automatica.

13.2 La conservazione dei dati personali per un periodo di tempo superiore a sette giorni, è ammessa esclusivamente su specifica richiesta dell'Autorità Giudiziaria o per lo svolgimento di attività di Polizia Giudiziaria.

14. Misure di sicurezza tecnologiche del sistema di videosorveglianza cittadino

14.1 L'Ente definisce le misure tecnologiche implementate al fine di proteggere la riservatezza, l'integrità e la disponibilità dei dati trattati mediante il sistema di videosorveglianza indicando:

a) l'architettura funzionale in cui siano indicati attori, sistemi e flussi informativi coinvolti nel trattamento;

b) le modalità di accesso, colloquio, trasmissione e fruizione del servizio da parte dei diversi attori;
c) i profili di autorizzazione e funzionalità offerte agli utenti del sistema;
d) le procedure di autenticazione informatica;
e) la tipologia di cifratura dei canali di trasmissione;
f) la sussistenza di procedure di backup e il loro aggiornamento e verifica;
g) le modalità di verifica periodica in ordine all'adeguatezza delle misure adottate;
h) l'implementazione di misure atte a rilevare, prevenire e rimuovere software maligni come virus, worm e trojan;
i) il processo di implementazione di aggiornamenti e patch;
j) le misure individuate per la protezione degli accessi fisici ai dispositivi e agli edifici per impedire accessi fisici non autorizzati;
k) gli strumenti utilizzati per monitorare la sicurezza dei sistemi;
l) l'eventuale isolamento di rete e segmentazione.

14.2 Sono implementati sistemi di videosorveglianza che consentano l'acquisizione di immagini chiare e dettagliate, in numero e con posizionamenti che comprimano quanto meno possibile i diritti e le libertà dei cittadini.

14.3 I sistemi di videosorveglianza devono essere scalabili, al fine di adattarsi alla crescita futura o ai cambiamenti nelle esigenze di sicurezza e con caratteristiche che consentano l'interoperabilità.

15. Informativa per il trattamento dei dati personali

15.1 In attuazione del principio di trasparenza, l'Ente Titolare rende nota ai cittadini la presenza di sistemi di videosorveglianza a mezzo di informativa cartellonistica

(informativa ridotta o di "primo livello") riportante gli elementi essenziali del trattamento, posizionata in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona videosorvegliata. L'Ente Titolare pubblica, sul proprio sito istituzionale, nella sua forma integrale e circostanziata, l'informativa per il trattamento dei dati personali che presenti i contenuti di cui all'art. 13 del GDPR oppure, ove applicabile, di cui all'art. 10 del D.lgs. 51/2018.

16. Sistemi integrati di videosorveglianza e accesso da parte delle Forze dell'Ordine

16.1 L'Ente Titolare promuove, in aderenza alle intese con il Comitato metropolitano di cui all'art. 6 del D.L. n. 14/2017 e/o con il Comitato provinciale per l'ordine e la sicurezza pubblica di cui all'art. 20 della L. 121/1981, il ricorso a sistemi integrati di videosorveglianza con altri soggetti pubblici.

16.2 L'Ente Titolare può fornire l'accesso al sistema di videosorveglianza alle Forze dell'Ordine che ne fanno richiesta.

16.3 E' esclusa la condivisione delle immagini del sistema di videosorveglianza a mezzo di applicazioni esterne al sistema e per le quali l'Ente Titolare non ha un contratto di fornitura in essere, con la previsione di specifiche misure tecniche e organizzative.

17. Censimento dei sistemi di videosorveglianza e collaborazione con privati

17.1 L'Ente Titolare può estendere, previo accordo e senza oneri economici, il proprio sistema di videosorveglianza, ricomprendendo i sistemi di soggetti privati impiegati per il controllo di spazi ed aree antistanti gli edifici privati secondo quanto previsto dal comma 1-bis dell'art. 7 del decreto-legge 20 febbraio 2017, n. 14 coordinato con la legge di conversione 18

aprile 2017, n. 48 recante: “Disposizioni urgenti in materia di sicurezza delle città”.

CAPO IV - Videosorveglianza per finalità di tutela del patrimonio o dei dipendenti/collaboratori e di protezione dei dati personali e dei sistemi informativi

18. La videosorveglianza per tutela di patrimonio e dipendenti

18.1 L'Ente Titolare installa, in attuazione dell’art. 32 del GDPR, sistemi di videosorveglianza al fine di tutelare il patrimonio, le persone, i dati personali e i sistemi informativi dell’Ente.

18.2 Le immagini raccolte tramite sistemi di videosorveglianza non possono in alcun modo essere utilizzate per controlli, anche se indiretti, sull’attività lavorativa del personale dell’Ente titolare.

18.3 Le telecamere installate negli atri, nelle portinerie e nei luoghi di accesso ai locali sono posizionate in modo da limitare l’inquadratura all’accesso stesso, senza possibilità di riprendere in alcun modo la registrazione ai “marcatempo” degli ingressi e delle uscite del personale né l’attività lavorativa degli addetti alle portinerie.

18.4 Non è ammessa l’installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all’attività lavorativa (per esempio bagni, spogliatoi, luoghi ricreativi, mense, ecc.).

18.5 Non è ammesso l'utilizzo di videocamere al solo fine di controllare il rispetto di divieti vari (es. divieto di fumare, di calpestare aiuole, di affiggere o fotografare) e comunque non sono ammessi controlli su ogni altra azione o comportamento non rispondente alle finalità al comma 1 del presente articolo. Dette finalità devono essere rese note attraverso apposita informativa.

18.6 I soggetti appositamente autorizzati e preposti al servizio di portineria e guardiania sono autorizzati alla consultazione delle immagini in tempo reale.

18.7 L'Ente Titolare installa il sistema di videosorveglianza per la finalità di cui al comma 1 del presente articolo, previo accordo collettivo stipulato con la rappresentanza sindacale, ai sensi dell'art. 4 dello Statuto dei lavoratori (L. n. 300/1970).

18.8 Agli interessati viene somministrata l'informativa per il trattamento dei dati personali nelle modalità indicate all'art. 15 del presente regolamento.

19. Ruoli e responsabilità

19.1 In aderenza alla deliberazione di cui all'art. 9.1 del presente regolamento, il Direttore dell'Ente è il Soggetto attuatore o Designato al trattamento, secondo il modello organizzativo adottato, ovvero il soggetto in capo al quale è riconosciuta la responsabilità dei trattamenti di dati personali effettuati a mezzo dei sistemi di videosorveglianza di cui all'articolo precedente.

19.2 In capo al soggetto di cui al comma precedente, sussiste l'onere di nominare, ai sensi e per gli effetti di cui all'art. 28 del GDPR, responsabili del trattamento i soggetti fornitori dei servizi correlati alla videosorveglianza.

19.3 Per gli aspetti tecnologici, in caso di utilizzo di sistemi e infrastrutture comunali, è Soggetto attuatore o Designato al trattamento, secondo il modello organizzativo adottato, il Responsabile dei sistemi informativi dell'Ente Titolare.

20. La consultazione dei dati

20.1 La consultazione dei dati registrati può essere effettuata soltanto:

a) per esigenze di manutenzione degli impianti;

b) per richieste effettuate dall'Autorità Giudiziaria e dalle Forze dell'Ordine;
c) in caso di danneggiamenti del patrimonio, furto di dati e danni a persone al fine di avviare le azioni, anche giudiziarie, di rimedio;
d) nel caso di visite ispettive da parte dell'Autorità Garante per la protezione dei dati personali;
e) in caso di richiesta di accesso dell'interessato ai propri dati personali;
f) in tempo reale e sino agli ultimi dieci minuti di registrazione da parte dei soggetti incaricati alla vigilanza.

21. Tempi di conservazione delle immagini

21.1 L'Ente Titolare configura il sistema di videosorveglianza in maniera da cancellare i dati personali automaticamente e con modalità tali da non rendere riutilizzabili i dati cancellati, dopo sette giorni.

21.2 Il periodo di conservazione di sette giorni è ritenuto necessario in ragione dell'importanza strategica del patrimonio informativo dell'Ente titolare e della rappresentanza politica dell'Ente.

22. Copie di dati e comunicazione

22.1 Il Soggetto attuatore o Designato al trattamento, secondo il modello organizzativo adottato, di cui all'art. 19 del presente regolamento può disporre l'effettuazione di copie dei dati registrati dal sistema di videosorveglianza soltanto in caso di specifica richiesta dell'Autorità Giudiziaria.

22.2 Le immagini sono condivise a mezzo del sistema di videosorveglianza oppure salvate su di un dispositivo rimovibile che, in caso di consegna differita rispetto all'effettuazione della copia, è custodito in maniera sicura.

23. Nuove installazioni, riposizionamento e rimozione delle apparecchiature di videosorveglianza

23.1 Il Soggetto attuatore o Designato al trattamento, secondo il modello organizzativo adottato, di cui all'art. 19 valuta la proporzionalità delle richieste di nuove installazioni, riposizionamento o rimozione delle apparecchiature di videosorveglianza agli scopi prefissati.

23.2 In caso di valutazione positiva, la richiesta è depositata presso le Rappresentanze sindacali per un periodo non inferiore a 20 giorni, trascorsi i quali, in mancanza di osservazioni da parte delle stesse, si considera acquisito il loro consenso alla nuova installazione o riposizionamento.

23.3 In caso di rimozione delle apparecchiature di videosorveglianza, il Soggetto attuatore o Designato al trattamento, secondo il modello organizzativo adottato, notizia le organizzazioni sindacali.

CAPO V - Aeromobili a pilotaggio remoto (droni)

24. Utilizzo dei droni

24.1 L'Ente Titolare può utilizzare i droni per le finalità di seguito indicate:

a) al fine di rilevazione di abusi edilizi e, più in generale, per ragioni connesse allo svolgimento di attività finalizzate a verifiche e sanzioni amministrative, laddove il rilevamento delle immagini sia immediato, diretto e contestuale alle suddette attività di polizia locale, non prolungato né sistematico;

b) per finalità di Protezione Civile, laddove il rilevamento delle immagini sia immediato, diretto e contestuale alle suddette attività di protezione civile e non implichi un trattamento di dati personali prolungato né sistematico.

24.2 Per la finalità di cui alla lettera a) del precedente comma è responsabile il dipendente che ha in uso il drone, che disciplina l'impiego dei dispositivi citati con apposito atto.

24.3 Per la finalità di cui alla lettera b) del comma 24.1 è responsabile il Direttore dell'Ente, che disciplina l'impiego dei dispositivi citati con apposito atto.

24.4 Il personale autorizzato all'utilizzo dei droni è addestrato e istruito sul loro utilizzo, anche riguardo agli aspetti legati alla protezione dei dati personali.

25. Il trattamento delle immagini registrate e i tempi di conservazione

25.1 Al termine del servizio il drone viene consegnato all'operatore autorizzato ai fini del salvataggio delle immagini a mezzo dell'applicativo in uso.

25.2 L'accesso a ciascuno dei file video deve essere specificamente autorizzato dai soggetti di cui ai punti 24.2 e 24.3, escludendo un'autorizzazione all'accesso massivo.

25.3 L'eventuale trasferimento delle immagini all'Autorità Giudiziaria deve avvenire con modalità che garantiscano l'accesso al solo personale autorizzato e la possibilità di verifica a posteriori dell'autenticità dei documenti.

25.4 Le immagini sono eliminate dal drone dopo il salvataggio di cui al comma 25.1 e sono cancellate da postazioni e piattaforma applicativa al massimo entro sei mesi, fatti salvi i casi di trasferimento ai sensi del comma precedente.

25.5 E' fatto salvo l'accesso alle immagini:

- per esigenze di manutenzione degli impianti;
- previa autorizzazione dell'Autorità di pubblica sicurezza e/o dell'Autorità giudiziaria, in caso di richiesta di accesso

dell'interessato ai propri dati personali, nonché ai sensi dell'art. 24 della L. n. 241/1990;

- nel caso di visite ispettive da parte dell'Autorità Garante per la protezione dei dati personali.

26. Misure di sicurezza tecnologiche del sistema

26.1 I soggetti di cui ai punti 24.2 e 24.3 sono responsabili dell'implementazione di misure di sicurezza di droni e piattaforma applicativa, tra cui:

a) l'implementazione di meccanismo utilizzato per tener traccia delle responsabilità (assegnazioni/acquisizione delle registrazioni, e degli accessi), c.d. watermarking;

b) l'utilizzo di tecniche che assicurano la non ripudiabilità delle registrazioni effettuate;

c) il tracciamento delle operazioni di visualizzazioni delle immagini;

d) la definizione di profili di autorizzazione distinti in base al ruolo assegnato a ciascun operatore;

e) l'accesso alle immagini è consentito solo a mezzo di postazioni connesse al dominio dell'Ente;

f) la registrazione di file di log non modificabili, relativi agli accessi e alle operazioni compiute dagli utenti;

g) l'utilizzo di tecniche di cifratura ai fini della conservazione delle immagini con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.