# PARCO ARCHEOLOGICO DI SEPINO – DIREZIONE REGIONALE MUSEI NAZIONALI MOLISE
# REGOLAMENTO
# IN MATERIA DI VIDEOSORVEGLIANZA

**Versione del documento**

| Versione | Data | Autore | Modifiche |
|---|---|---|---|
| **1.0** | Da definire in sede di approvazione | Parco archeologico di Sepino – Direzione regionale Musei nazionali Molise | Personalizzazione del modello MiC |

## Sommario

**Premessa** ..... 3
**Articolo 1 – Riferimenti Normativi e Linee guida** ..... 3
**Articolo 2 – Campo di applicazione e Definizioni** ..... 4
**Articolo 3 – Principi generali** ..... 6
**Articolo 4 – Finalità e basi giuridiche** ..... 8
**Articolo 5 – Gestione dei sistemi di videosorveglianza e ruoli privacy** ..... 9
**Articolo 6 – Misure di sicurezza** ..... 10
**Articolo 7 - Valutazione di impatto sulla protezione dei dati (DPIA)** ..... 13
**Articolo 8 - Conservazione delle immagini e limiti temporali** ..... 13
**Articolo 9 - Procedura per l'accesso alle immagini** ..... 14
**Articolo 10 - Limiti di utilizzo della videosorveglianza** ..... 16
**Articolo 11 – Rapporti con l'Arma dei Carabinieri e la Polizia di StatoErrore. Il segnalibro non è definito.**
**Articolo 12 – Trasparenza informativa** ..... 16
**Articolo 13 – Diritti degli interessati** ..... 17
**Articolo 14 – Norme di rinvio** ..... 18

## Premessa

Il Ministero della Cultura (di seguito "Ministero" o "MiC"), nell'ambito delle proprie funzioni istituzionali di tutela, conservazione e valorizzazione del patrimonio culturale nazionale, assicura adeguati livelli di sicurezza delle persone, delle strutture e dei beni pubblici affidati alla propria responsabilità.
Le sedi e le strutture del Ministero comprendono uffici amministrativi, direzioni, archivi e depositi documentali, locali tecnici e infrastrutture di supporto, nonché istituti e luoghi della cultura – quali musei, biblioteche, archivi di Stato e complessi monumentali – nei quali sono custoditi beni di rilevante valore storico, artistico e culturale.
In tale contesto, ciascuna struttura del Ministero della Cultura, per il tramite dell'esercente le funzioni di Titolare del trattamento, può adottare sistemi di videosorveglianza presso gli accessi alle sedi istituzionali, nelle aree perimetrali degli edifici, negli spazi destinati alla fruizione pubblica e, ove strettamente necessario, in specifici ambienti interni caratterizzati da particolari esigenze di sicurezza o di tutela del patrimonio culturale.
L'installazione e l'utilizzo dei sistemi di videosorveglianza sono finalizzati alla tutela dell'incolumità del personale, dei visitatori e degli utenti dei luoghi della cultura, alla prevenzione e al contrasto di atti illeciti o danneggiamenti, alla protezione delle infrastrutture e degli impianti, nonché alla salvaguardia del patrimonio culturale e immobiliare affidato alla responsabilità della struttura.
Si precisa che le immagini che consentono l'identificazione, diretta o indiretta, di persone fisiche costituiscono dati personali ai sensi della normativa vigente in materia di protezione dei dati personali. L'utilizzo dei sistemi di videosorveglianza comporta pertanto un trattamento di dati personali che può incidere sul diritto alla protezione dei dati e sulla riservatezza dei soggetti eventualmente presenti nelle aree oggetto di ripresa.
Il presente regolamento disciplina il funzionamento e la gestione dei sistemi di videosorveglianza, assicurando che il trattamento dei dati personali effettuato mediante tali sistemi avvenga nel pieno rispetto della normativa europea e nazionale in materia di protezione dei dati personali, nonché dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riguardo alla dignità, alla riservatezza e all'identità personale.

## Articolo 1 – Riferimenti Normativi e Linee guida

- Decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»
- Provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010 – Provvedimento in materia di videosorveglianza;

- Regolamento Generale sulla Protezione dei Dati Personali - Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Legge 20 maggio 1970, n. 300 “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell’attività sindacale nei luoghi di lavoro e norme sul collocamento” (G.U. 27 maggio 1970, n. 131);
- Decreto Legislativo n. 151 del 14 settembre 2015, art. 23 recante modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196;
- Decreto legislativo 10 agosto 2018, n. 101 - 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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15 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;
- Decreto legislativo 18 maggio 2018, n. 51 (di seguito: “Decreto”), recante l’attuazione della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonchè alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio
- Linee guida 3/2019 sul trattamento di dati attraverso apparecchiature video, adottate dal Comitato Europeo per la protezione dei dati il 29/01/2020 (EDPB - *Guidelines 3/2019 on processing of personal data through video devices*)

## Articolo 2 – Campo di applicazione e Definizioni

1. 1. Il presente Regolamento disciplina il trattamento dei dati personali effettuato mediante sistemi di videosorveglianza installati presso il Parco archeologico di Sepino – Direzione regionale Musei nazionali Molise, nelle sedi e nei luoghi della cultura di propria competenza. Ai fini del presente Regolamento, il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato nell’ambito delle competenze istituzionali della struttura, sotto

la responsabilità dell'**esercente le funzioni di Titolare del trattamento**, individuato secondo l'assetto organizzativo dell'Amministrazione e nel rispetto delle disposizioni di cui al **Decreto Ministeriale 30 gennaio 2026, n. 49**, recante disposizioni in materia di organizzazione e governance della protezione dei dati personali nell'ambito del Ministero della Cultura.

Le disposizioni del presente Regolamento si applicano a qualsiasi sistema di videosorveglianza, analogico o digitale, nonché a ogni dispositivo idoneo alla ripresa, registrazione, trasmissione o memorizzazione di immagini installato presso gli spazi della struttura, quali accessi alle sedi istituzionali, aree perimetrali degli edifici, ambienti interni, spazi destinati alla fruizione pubblica e, ove presenti, luoghi della cultura quali musei, archivi, biblioteche, complessi monumentali o aree espositive.
Nell'ambito dell'organizzazione della struttura, l'**esercente le funzioni di Titolare del trattamento** provvede, ove necessario, alla designazione di uno o più **Designati al trattamento dei dati personali**, ai sensi dell'articolo 2-quaterdecies del decreto legislativo 30 giugno 2003, n. 196 e dell'articolo 2 del **D.M. n. 49/2026**, ai quali possono essere attribuiti specifici compiti di gestione, coordinamento e supervisione dei sistemi di videosorveglianza, nel rispetto delle istruzioni impartite dal Titolare e della normativa vigente in materia di protezione dei dati personali.
Il presente Regolamento si applica altresì ai sistemi di videosorveglianza gestiti, in tutto o in parte, da soggetti esterni incaricati di attività di vigilanza, manutenzione, gestione tecnica o supporto operativo degli impianti, i quali operano, ove previsto, in qualità di **responsabili del trattamento** ai sensi dell'articolo 28 del Regolamento (UE) 2016/679.

2. Ai fini del presente Regolamento si intende per:

- **«dato personale»**, qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo quali nome, numero di identificazione, dati relativi all'ubicazione, identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **«trattamento»**, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **«banca dati»**, il complesso organizzato di dati personali costituito dalle registrazioni e dalle immagini acquisite tramite i sistemi di videosorveglianza installati presso le sedi del Ministero, riferite prevalentemente ai soggetti che accedono o transitano nelle aree oggetto di ripresa;
- **«profilazione»**, qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, il comportamento, l'ubicazione o gli spostamenti della medesima;

- **«pseudonimizzazione»**, il trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, conservate separatamente e soggette a misure tecniche e organizzative idonee a garantirne la non attribuibilità a una persona fisica identificata o identificabile;
- **«titolare del trattamento»**, il Ministero, quale autorità pubblica che determina le finalità e i mezzi del trattamento dei dati personali effettuato mediante sistemi di videosorveglianza;
- **«responsabile del trattamento»**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (quali, a titolo esemplificativo, società di vigilanza o manutentori degli impianti);
- **«soggetto autorizzato al trattamento»**, la persona fisica che, sotto l'autorità del titolare o del responsabile, è formalmente autorizzata ad accedere ai dati personali e a compiere operazioni di trattamento nell'ambito delle proprie mansioni;
- **«interessato»**, la persona fisica cui si riferiscono i dati personali oggetto di trattamento, ivi compresi dipendenti, collaboratori, visitatori, utenti, fornitori o altri soggetti che accedono alle sedi ministeriali;
- **«terzo»**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo diverso dall'interessato, dal titolare, dal responsabile del trattamento e dai soggetti autorizzati al trattamento;
- **«violazione dei dati personali»**, la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **«comunicazione»**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante messa a disposizione o consultazione;
- **«diffusione»**, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante messa a disposizione o consultazione;
- **«dato anonimo»**, il dato che non può essere associato a un interessato identificato o identificabile, né direttamente né indirettamente;
- **«DPO»**, il Responsabile della Protezione dei Dati personali (Data Protection Officer), designato dal Ministero ai sensi dell'articolo 37 del Regolamento (UE) 2016/679.

## Articolo 3 – Principi generali

1. La raccolta, la registrazione, la conservazione, la consultazione e, in generale, qualsiasi utilizzo delle immagini acquisite mediante i sistemi di videosorveglianza configurano un trattamento di dati personali ai sensi della normativa vigente.
2. Il trattamento dei dati personali mediante sistemi di videosorveglianza avviene esclusivamente nell'ambito dello svolgimento delle proprie funzioni istituzionali, con particolare riferimento alla tutela del patrimonio patrimoni, immobiliare e museale, nonché alla prevenzione di atti illeciti, alla protezione delle sedi centrali e periferiche, e delle infrastrutture strategiche.

3. La determinazione della dislocazione delle telecamere, delle modalità di ripresa, dei tempi di conservazione e delle modalità di trattamento dei dati raccolti è effettuata nel rispetto dei seguenti principi:

**a) Principio di liceità**

Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato nel rispetto del principio di liceità di cui all'articolo 5 del Regolamento (UE) 2016/679.
In particolare, tale trattamento trova la propria base giuridica nell'articolo 6, paragrafo 1, lettera e), del medesimo Regolamento, in quanto necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri attribuiti al Ministero della Cultura.
Il trattamento è effettuato, nell'ambito delle competenze istituzionali della struttura che adotta il presente regolamento, sotto la responsabilità dell'**esercente le funzioni di Titolare del trattamento**, nel rispetto della normativa europea e nazionale in materia di protezione dei dati personali, nonché delle disposizioni vigenti in materia di sicurezza delle sedi istituzionali e di tutela del patrimonio pubblico e culturale.
Restano in ogni caso ferme, ove applicabili, le **procedure di garanzia previste dall'articolo 4 della legge 20 maggio 1970, n. 300**, in materia di utilizzo di impianti audiovisivi e di altri strumenti dai quali possa derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori.

**b) Principio di necessità e minimizzazione**
In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), del Regolamento (UE) 2016/679, i sistemi di videosorveglianza, le infrastrutture tecnologiche e i software utilizzati sono configurati in modo da **ridurre al minimo** l'utilizzo di dati personali e identificativi.
Il trattamento è limitato ai soli dati strettamente necessari per il perseguimento delle finalità istituzionali. Deve essere escluso ogni uso superfluo o eccedente, nonché evitati eccessi e ridondanze nell'installazione o nel posizionamento delle telecamere.
Qualora le finalità perseguite possano essere realizzate senza l'identificazione degli interessati, i sistemi sono configurati per privilegiare riprese di insieme, limitando l'angolo visuale alle sole aree effettivamente da proteggere ed evitando, ove possibile, l'acquisizione di immagini dettagliate non necessarie.
I sistemi informatici sono altresì configurati per la cancellazione automatica delle registrazioni decorso il periodo di conservazione stabilito.

**c) Principio di proporzionalità**
La raccolta e l'utilizzo delle immagini devono risultare proporzionati agli scopi perseguiti e commisurati al grado di rischio concreto presente nelle aree oggetto di ripresa.
Gli impianti di videosorveglianza possono essere attivati esclusivamente quando altre misure di sicurezza, quali sistemi di controllo accessi, vigilanza fisica, sistemi di allarme o protezioni strutturali, siano state valutate come insufficienti o non pienamente idonee a garantire il livello di tutela richiesto.

In particolare, l'installazione delle telecamere deve essere giustificata dalla necessità di proteggere aree sensibili, ambienti istituzionali, locali tecnici, archivi, autorimesse, spazi museali o sedi caratterizzate da specifiche esigenze di sicurezza.
Nell'uso delle apparecchiature destinate alla ripresa di aree esterne ed edifici, il trattamento deve avvenire con modalità tali da limitare l'angolo di visuale alla sola area effettivamente da proteggere, evitando riprese eccedenti di spazi pubblici o aree non pertinenti.
La proporzionalità deve essere valutata in ogni fase del trattamento, dalla progettazione del sistema alla sua gestione operativa.

**d) Principio di limitazione della finalità**
Ai sensi dell'articolo 5, paragrafo 1, lettera b), del Regolamento (UE) 2016/679, i dati personali sono raccolti per finalità determinate, esplicite e legittime e sono successivamente trattati in modo non incompatibile con tali finalità.
Le immagini non possono essere utilizzate per finalità diverse da quelle istituzionali di sicurezza e tutela del patrimonio, né per forme di controllo sistematico e generalizzato dell'attività lavorativa del personale.

## Articolo 4 – Finalità e basi giuridiche

### 1. Finalità del trattamento

L'installazione e l'utilizzo dei sistemi di videosorveglianza rispondono a finalità determinate, esplicite e legittime, riconducibili alle funzioni istituzionali dell'Amministrazione, ed in particolare:

a) **tutela del patrimonio pubblico**, immobiliare, mobiliare, documentale, archivistico e museale, ivi compresi i beni di interesse storico e culturale custoditi presso le sedi ministeriali;

b) **tutela della sicurezza delle persone** che, a vario titolo, accedono o operano presso le sedi del Ministero (personale dipendente, autorità politiche, collaboratori, visitatori, fornitori), nonché prevenzione e contrasto di atti illeciti, danneggiamenti, intrusioni, aggressioni o minacce alla sicurezza delle strutture;

c) **adempimento a specifiche richieste dell'Autorità Giudiziaria o di Polizia Giudiziaria**, nell'ambito di procedimenti investigativi o giudiziari.

Le immagini raccolte non possono essere utilizzate per finalità diverse o incompatibili con quelle sopra indicate.

## Articolo 5 – Gestione dei sistemi di videosorveglianza e ruoli privacy

1. I sistemi di videosorveglianza installati presso la struttura sono gestiti nell'ambito delle competenze istituzionali dell'Amministrazione, sotto la responsabilità dell'**esercente le funzioni di Titolare del trattamento**, individuato secondo l'assetto organizzativo del Ministero della Cultura e nel rispetto delle disposizioni di cui al **Decreto Ministeriale 30 gennaio 2026, n. 49**.

Titolare del trattamento: Ministero della Cultura, via del Collegio Romano 27, 00186 Roma. Le relative funzioni presso il Parco archeologico di Sepino – Direzione regionale Musei nazionali Molise sono esercitate dal Direttore, dott. Enrico Rinaldi, con sede in Contrada Altilia 1, 86017 Sepino (CB). Recapiti dell'Istituto: PEO pa-sepino-mu-cb@cultura.gov.it; PEC pa-sepino-mu-cb@pec.cultura.gov.it; telefono della sede di Sepino +39 0874 790207 e della Direzione regionale +39 0874 431386.

**Responsabile della protezione dei dati** (RPD/DPO) del MiC: rpd@cultura.gov.it; PEC rpd@pec.cultura.gov.it. **Referente privacy dell'Istituto**: pa-sepino.privacy@cultura.gov.it; telefono +39 0874 431386.

Il Dott. Emilio Morrone è individuato quale **Soggetto autorizzato al trattamento dei dati personali mediante sistemi di videosorveglianza e alla gestione e manutenzione tecnica dei relativi impianti**, in forza del provvedimento di nomina sottoscritto dal Direttore dell'Istituto e acquisito al protocollo MIC_PA-SEPINO-MU-CB n. 0002914-A dell'11 maggio 2026.

L'autorizzazione si estende a tutti i luoghi della cultura afferenti al Parco archeologico di Sepino – Direzione regionale Musei nazionali Molise e comprende le operazioni espressamente indicate nel provvedimento, da svolgersi nei limiti delle finalità istituzionali e delle istruzioni impartite.

La posizione del soggetto autorizzato è ricondotta alla disciplina di cui agli articoli 3 e 9 del D.M. 30 gennaio 2026, n. 49, ferma restando la distinta figura del Designato al trattamento disciplinata dall'articolo 8 del medesimo decreto.

2. L'esercente le funzioni di Titolare del trattamento può individuare uno o più **Designati al trattamento dei dati personali** ai sensi dell'articolo 2-quaterdecies del decreto legislativo 30 giugno 2003, n. 196 e del D.M. n. 49/2026, ai quali sono attribuiti specifici compiti di gestione, coordinamento e supervisione dei sistemi di videosorveglianza, nel rispetto delle istruzioni impartite dal Titolare e della normativa vigente in materia di protezione dei dati personali.

3. Qualora attività di telecontrollo, monitoraggio remoto, manutenzione tecnica, gestione applicativa o supporto operativo dei sistemi di videosorveglianza siano affidate a soggetti esterni, l'esercente le funzioni di Titolare del trattamento provvede alla designazione del soggetto affidatario quale **Responsabile del trattamento**, ai sensi dell'articolo 28 del Regolamento (UE) 2016/679, mediante apposito atto giuridico o clausola contrattuale che disciplini, tra l'altro, gli obblighi di sicurezza, riservatezza, tracciabilità degli accessi, gestione degli incidenti e restituzione o cancellazione dei dati.
4. Il **Designato al trattamento** provvede a individuare e designare per iscritto i **Soggetti autorizzati al trattamento dei dati personali**, ossia le persone fisiche che, in ragione delle proprie mansioni, sono abilitate:

- ad accedere ai locali nei quali sono collocate le postazioni di controllo o i dispositivi di registrazione (DVR/NVR);
- ad utilizzare i sistemi di monitoraggio delle immagini in tempo reale;
- nei soli casi in cui ciò sia strettamente necessario per il perseguimento delle finalità istituzionali, a consultare, visionare ed estrarre le immagini registrate.

5. Il Designato definisce livelli differenziati di autorizzazione e accesso ai sistemi di videosorveglianza, in relazione alle specifiche funzioni attribuite a ciascun soggetto, distinguendo in particolare:

- il personale abilitato esclusivamente alla visione in tempo reale delle immagini;
- il personale autorizzato, a determinate condizioni e secondo procedure formalizzate, ad effettuare operazioni ulteriori quali registrazione, copia, esportazione, cancellazione o messa a disposizione delle immagini nei casi consentiti dalla legge.

6. Le autorizzazioni e i profili di accesso ai sistemi sono configurati nel rispetto dei principi di **limitazione degli accessi, minimizzazione e segregazione delle funzioni**, assicurando la tracciabilità delle operazioni effettuate sui sistemi e sulle registrazioni.
7. I Designati e i Soggetti autorizzati al trattamento sono tenuti al rigoroso rispetto degli obblighi di **riservatezza e sicurezza dei dati**, alla diligente custodia delle credenziali di accesso e alla corretta gestione e conservazione delle immagini eventualmente estratte, nonché all'osservanza delle istruzioni impartite dall'esercente le funzioni di Titolare del trattamento e delle disposizioni contenute nel presente Regolamento.

## Articolo 6 – Misure di sicurezza

Gli impianti di videoripresa e i dati personali con essi raccolti devono essere salvaguardati mediante adeguate e preventive misure tecniche e organizzative, idonee a ridurre al minimo i rischi di distruzione, perdita, anche accidentale, accesso non autorizzato, trattamento non consentito o non

conforme alle finalità per le quali i dati sono stati raccolti, anche con riferimento alla trasmissione e remotizzazione delle immagini.

Configurazione tecnica: telecamere con registrazione locale su NVR/DVR in locali o armadi ad accesso limitato; visualizzazione in tempo reale presso le sale regia dei siti; trasporto dei flussi video su rete dedicata e segregata rispetto agli altri sistemi informatici.

Sono adottate tutte le misure di sicurezza ritenute adeguate, ai sensi del Regolamento (UE) 2016/679, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

A tal fine, sono adottate, tra le altre, le seguenti misure:

1. **Protezione fisica dei locali di controllo**

   I locali nei quali sono collocati i sistemi di visualizzazione (sale regia, postazioni di controllo, locali tecnici) sono protetti contro l'accesso non autorizzato. L'accesso è consentito esclusivamente ai Designati e ai Soggetti autorizzati al trattamento, nonché, per esigenze tecniche, ai soggetti esterni incaricati della manutenzione, formalmente nominati Responsabili del trattamento con funzioni di Amministratore di Sistema.

2. **Sistema di autenticazione informatica**

   È predisposto un sistema di controllo degli accessi basato su credenziali individuali (user-id e password o sistemi equivalenti), con profili di autorizzazione differenziati in relazione alle mansioni svolte (es. sola visione live, accesso alle registrazioni, estrazione delle immagini, manutenzione tecnica).

3. **Presenza durante interventi tecnici esterni**

   Le eventuali verifiche o interventi tecnici effettuati da personale esterno sono svolti, ove possibile, alla presenza di personale interno autorizzato.

4. **Limitazione degli accessi alle registrazioni**

   Nei sistemi configurati per la registrazione e conservazione delle immagini, è limitata la possibilità per i soggetti abilitati alla sola visione "live" di accedere alle registrazioni differite o di effettuare operazioni di cancellazione, duplicazione o esportazione.

5. **Tracciabilità degli accessi (access log)**

   Sono adottati sistemi di registrazione degli accessi logici ai sistemi informatici e agli archivi elettronici, con tracciamento delle operazioni compiute sulle immagini (visualizzazione, esportazione, cancellazione), comprensive di riferimento temporale.
   I log sono conservati per un periodo congruo rispetto alle esigenze di verifica interna e comunque non inferiore a sei mesi, garantendone completezza, inalterabilità e integrità.

6. **Osservanza del Regolamento**

   I soggetti autorizzati sono tenuti al rigoroso rispetto del presente Regolamento, con particolare riguardo al principio di pertinenza e non eccedenza dei dati trattati.

7. **Cancellazione automatica delle registrazioni**

   I sistemi sono configurati per la cancellazione automatica delle registrazioni allo scadere del termine di conservazione previsto. La cancellazione avviene preferibilmente mediante sovrascrittura automatica del supporto.

8. **Distruzione dei supporti obsoleti**

   In caso di sostituzione dei supporti di memorizzazione per usura o aggiornamento tecnologico, i supporti dismessi sono distrutti o resi definitivamente inutilizzabili mediante procedure idonee a impedire il recupero dei dati.

9. **Cancellazione in ambiente controllato**

   Le operazioni di cancellazione manuale o distruzione dei supporti sono effettuate esclusivamente in ambiente controllato, presso le sedi ministeriali.

10. **Anonimizzazione esterna dei supporti**

    I supporti di memorizzazione non riportano all'esterno indicazioni nominative o dati idonei a identificare direttamente gli interessati eventualmente ripresi.

11. **Cifratura delle registrazioni**

    Ove tecnicamente possibile, sono adottati sistemi di cifratura delle registrazioni e delle comunicazioni tra dispositivi di ripresa, server di archiviazione e postazioni di monitoraggio.

12. **Protezione fisica dei server/DVR/NVR**

    I dispositivi di registrazione sono custoditi all'interno di armadi rack chiusi a chiave o in locali tecnici protetti. Le chiavi o le credenziali di accesso sono custodite dai Designati o dai Soggetti autorizzati.

13. **Protezione dei locali tecnici**

    I locali che ospitano i rack o i server sono chiusi a chiave e accessibili esclusivamente ai soggetti autorizzati.

14. **Posizionamento dei monitor**

    I monitor delle postazioni di videosorveglianza sono collocati in modo da evitare la visione, anche occasionale, delle immagini da parte di soggetti non autorizzati.

15. **Alimentazione protetta**

I sistemi di registrazione sono alimentati mediante gruppi di continuità (UPS) o sistemi equivalenti, idonei a garantire la protezione da interruzioni improvvise di energia elettrica.

Qualora siano utilizzati apparati digitali connessi a reti informatiche interne o pubbliche, gli stessi sono adeguatamente protetti contro i rischi di accesso abusivo mediante firewall, segmentazione di rete, autenticazione forte e aggiornamenti periodici di sicurezza.

La trasmissione di immagini tramite reti pubbliche di comunicazione, nonché tramite connessioni wireless (ad es. GPRS, Wi-Fi o altre tecnologie equivalenti), avviene esclusivamente previa applicazione di tecniche crittografiche idonee a garantirne la riservatezza e l'integrità.

## Articolo 7 - Valutazione di impatto sulla protezione dei dati (DPIA)

Qualora, in considerazione della natura, dell'ambito di applicazione, del contesto o delle finalità del trattamento effettuato mediante sistemi di videosorveglianza, possano derivare **rischi elevati per i diritti e le libertà delle persone fisiche**, è effettuata una **Valutazione di Impatto sulla Protezione dei Dati (DPIA)** ai sensi dell'articolo 35 del Regolamento (UE) 2016/679.

In particolare, la DPIA è condotta nei casi in cui il trattamento presenti caratteristiche tali da comportare un rischio elevato, anche con riferimento, a titolo esemplificativo, alla videosorveglianza sistematica di aree accessibili al pubblico, alla presenza di lavoratori nelle aree oggetto di ripresa, alla sorveglianza di aree caratterizzate da particolare sensibilità istituzionale, nonché all'utilizzo di sistemi di monitoraggio remoto o di trasmissione delle immagini tramite reti di comunicazione.

La valutazione di impatto è effettuata **prima dell'attivazione o della modifica sostanziale del sistema di videosorveglianza** dall'esercente le funzioni di Titolare del trattamento o suo Designato, previa consultazione del Responsabile della protezione dei dati (DPO), ove richiesto dalla normativa vigente.

Qualora dalla valutazione emerga che il trattamento presenterebbe un rischio elevato residuo per i diritti e le libertà degli interessati in assenza di misure adeguate di mitigazione, si procede, ove necessario, alla **consultazione preventiva dell'Autorità Garante per la protezione dei dati personali**, ai sensi dell'articolo 36 del Regolamento (UE) 2016/679.

## Articolo 8 - Conservazione delle immagini e limiti temporali

Nei sistemi che prevedono la registrazione delle immagini, la conservazione delle stesse avviene nel rispetto dei principi di proporzionalità, necessità e limitazione della conservazione.

Tenuto conto delle finalità dei sistemi di videosorveglianza installati presso le sedi del Ministero, del livello di rischio valutato in misura medio/alta per talune aree (ivi comprese aree perimetrali, ambienti istituzionali sensibili, locali tecnici, autorimesse e spazi museali), nonché delle esigenze connesse a festività e periodi di chiusura degli uffici, le immagini sono conservate per un periodo di **168 ore.** Solo in presenza di particolari esigenze motivate o in caso del verificarsi di specifici eventi, quali, a titolo esemplificativo:

- necessità di monitorare con continuità zone non presidiate;

- aree caratterizzate da significativo afflusso di pubblico;
- rischio concreto di furto, danneggiamento o altri illeciti con difficoltà di tempestiva segnalazione;
- eventi istituzionali o situazioni eccezionali che comportino un incremento del livello di rischio,

il termine di conservazione può essere esteso per un **periodo non superiore a sette giorni**, salvo diversa e specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria, che legittimi una conservazione ulteriore per finalità investigative.

Il sistema di registrazione è programmato in modo da garantire l'integrale cancellazione automatica delle immagini allo scadere del termine previsto, anche mediante sovrascrittura, con modalità tecniche tali da rendere i dati cancellati non riutilizzabili.

Il **Designato al trattamento per la videosorveglianza**, individuato dall'esercente le funzioni di Titolare, è responsabile della corretta conservazione delle registrazioni e della programmazione delle tempistiche di registrazione e cancellazione delle immagini, secondo quanto stabilito nel presente Regolamento.

Tali compiti possono essere affidati, per specifiche attività tecniche, a soggetti terzi formalmente designati quali Responsabili del trattamento ai sensi dell'articolo 28 del Regolamento (UE) 2016/679.

Il mancato rispetto dei termini massimi di conservazione, dell'obbligo di cancellazione automatica e delle misure di sicurezza previste può comportare l'applicazione delle sanzioni amministrative previste dall'articolo 83 del Regolamento (UE) 2016/679, oltre alle eventuali responsabilità disciplinari e contabili.

Le registrazioni delle immagini sono custodite in locali tecnici o sale di controllo protette, chiuse a chiave o con sistemi equivalenti di sicurezza, accessibili esclusivamente ai soggetti formalmente designati e autorizzati.

In conformità alla normativa vigente e alle finalità istituzionali del sistema, nessun dipendente o altro soggetto può accedere direttamente alle immagini registrate al di fuori dei ruoli e delle procedure previste dal presente Regolamento, anche qualora le stesse riguardino eventi di personale interesse (ad esempio, danneggiamento o furto del proprio veicolo all'interno di aree ministeriali).

In tali casi, l'accesso alle immagini potrà avvenire esclusivamente su richiesta e per il tramite dell'Autorità Giudiziaria o della Polizia Giudiziaria, nei limiti e secondo le modalità previste dalla legge.

## Articolo 9 - Procedura per l'accesso alle immagini

1. Considerato che l'accesso alle videoregistrazioni costituisce trattamento di dati personali ai sensi dell'articolo 4 del Regolamento (UE) 2016/679, i supporti di registrazione e le immagini in essi contenute possono essere messi a disposizione esclusivamente su richiesta motivata:

- delle Strutture competenti del Ministero, per esigenze istituzionali connesse alla tutela del patrimonio culturale;
- dell'Autorità Giudiziaria o della Polizia Giudiziaria, nell'ambito di attività investigative o procedimenti giudiziari;
- degli interessati che intendano esercitare i diritti di cui agli articoli 15-22 del Regolamento (UE) 2016/679, nei limiti e secondo le modalità previste dalla normativa vigente.

2. La richiesta di cui al comma 1 deve essere indirizzata al soggetto Designato al trattamento competente per la sede interessata, ai fini dell'individuazione degli autori di eventuali fatti illeciti a danno del Ministero o di altri soggetti, in situazioni di emergenza o necessità che giustifichino l'accesso ai dati, ovvero per l'esercizio dei diritti dell'interessato.

3. Le richieste di visualizzazione o acquisizione delle immagini devono possedere le seguenti caratteristiche:

   - provenire da soggetti legittimati;
   - essere formulate per iscritto, ovvero in altra forma documentabile e tracciabile;
   - essere adeguatamente motivate, con indicazione delle ragioni della richiesta;
   - essere circoscritte quanto più possibile sotto il profilo temporale e spaziale (data, fascia oraria, luogo dell'evento).

4. Qualora la richiesta risulti incompleta o priva dei requisiti sopra indicati, il Designato al trattamento richiede le necessarie integrazioni istruttorie prima di fornire riscontro.

5. Il Designato accerta preliminarmente l'effettiva esistenza delle immagini richieste, tenuto conto dei termini di conservazione previsti dal presente Regolamento, e ne dà comunicazione al richiedente. In caso positivo, qualora sia autorizzata la sola visione, il Designato stabilisce il giorno, l'ora e il luogo in cui l'interessato o il soggetto legittimato potrà visionare esclusivamente le immagini oggetto di autorizzazione, adottando ogni misura idonea a tutelare i diritti di eventuali terzi ripresi.

6. L'eventuale estrazione o copia delle videoregistrazioni avviene esclusivamente nei casi consentiti dalla legge e secondo procedure formalizzate, garantendo la tracciabilità delle operazioni effettuate e la corretta conservazione del supporto consegnato.

7. Le richieste di esercizio dei diritti in materia di protezione dei dati personali sono indirizzate agli esercenti le funzioni di Titolare o designati, ai recapiti ufficiali pubblicati sul sito internet istituzionale del Ministero ovvero direttamente al Responsabile della protezione dei dati.

8. È in ogni caso esclusa la possibilità per dipendenti o altri soggetti non espressamente autorizzati di accedere direttamente alle immagini registrate, anche qualora le stesse riguardino eventi di personale interesse. L'eventuale accesso per finalità giudiziarie avviene esclusivamente per il tramite dell'Autorità Giudiziaria o della Polizia Giudiziaria.

## Articolo 10 - Limiti di utilizzo della videosorveglianza

1. Le immagini raccolte mediante i sistemi di videosorveglianza non possono essere utilizzate per finalità diverse da quelle espressamente indicate nel presente Regolamento e, in particolare, per scopi ulteriori rispetto a quelli istituzionali di sicurezza, tutela del patrimonio pubblico e prevenzione di atti illeciti.
2. Gli impianti di videosorveglianza non possono essere utilizzati, ai sensi dell'articolo 4 della legge 20 maggio 1970, n. 300, per effettuare controlli sull'attività lavorativa dei dipendenti.
3. È esclusa qualsiasi forma di controllo sistematico e generalizzato delle prestazioni lavorative. Eventuali utilizzi indiretti delle immagini sono consentiti esclusivamente nei limiti e secondo le garanzie previste dalla normativa vigente.
4. Ai sensi dell'articolo 4, comma 1, della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio pubblico. Pertanto, qualora i sistemi di videosorveglianza comportino, anche solo potenzialmente, la possibilità di controllo a distanza dell'attività dei lavoratori, la loro installazione è subordinata alla preventiva stipula di un accordo collettivo con la rappresentanza sindacale unitaria o con le rappresentanze sindacali aziendali competenti.
5. In mancanza di accordo sindacale, l'installazione degli impianti è subordinata al rilascio di apposita autorizzazione da parte della sede territoriale dell'Ispettorato Nazionale del Lavoro ovvero, nei casi previsti dalla normativa vigente, della sede centrale del medesimo Ispettorato.
6. Resta fermo che i sistemi di videosorveglianza non sono installati né utilizzati per finalità di controllo sistematico e generalizzato dell'attività lavorativa del personale, ma esclusivamente per le finalità istituzionali di sicurezza e tutela del patrimonio pubblico indicate nel presente Regolamento.

## Articolo 11 – Trasparenza informativa

L'esercente le funzioni di titolare o suoi designati, garantiscono indicazioni chiare e trasparenti alle persone che possono essere riprese dai sistemi di videosorveglianza, al fine di informarle della presenza delle telecamere e delle modalità del trattamento dei dati personali.

L'obbligo di informativa, ai sensi dell'art.13 del Regolamento (UE) 2016/679, è adempiuto mediante modalità semplificata, attraverso l'esposizione di appositi cartelli recanti l'indicazione della presenza di uno o più impianti di videosorveglianza. I cartelli:

- sono collocati prima dell'accesso all'area oggetto di ripresa o comunque in posizione chiaramente visibile rispetto all'area monitorata;
- hanno dimensioni e caratteristiche grafiche tali da garantirne la leggibilità anche in condizioni di scarsa illuminazione;
- indicano in modo esplicito se l'attività è limitata alla sola ripresa o si estende anche alla registrazione delle immagini.

L'informativa di primo livello contiene almeno:

- l'identità e i dati di contatto del Titolare del trattamento;
- i dati di contatto del Responsabile della Protezione dei Dati (DPO);
- le finalità del trattamento;
- la base giuridica;
- il periodo di conservazione delle immagini;
- il riferimento ai diritti riconosciuti agli interessati.

L'informativa di primo livello rinvia all'informativa di dettaglio (secondo livello), resa disponibile sul sito internet istituzionale, mediante indicazione dell'URL o tramite QR code riportato sul cartello.

Il personale dipendente è informato in merito alle finalità, alle modalità e ai limiti del trattamento dei dati personali effettuato mediante sistemi di videosorveglianza, anche tramite comunicazioni interne, pubblicazione sulla intranet istituzionale o altre modalità idonee a garantirne la piena conoscibilità.

## Articolo 12 – Diritti degli interessati

**1.** In relazione al trattamento dei dati personali effettuato mediante i sistemi di videosorveglianza, l'interessato può esercitare i diritti previsti dagli **articoli 15 e seguenti del Regolamento (UE) 2016/679**, nei limiti e secondo le modalità previste dalla normativa vigente.

In particolare, l'interessato ha il diritto di:

- ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di **accedere alle immagini che lo coinvolgono**, nei limiti della tutela dei diritti e delle libertà di terzi eventualmente ripresi;
- ricevere informazioni in merito alle **finalità del trattamento, alle categorie di dati trattati, ai destinatari o alle categorie di destinatari, al periodo di conservazione delle immagini e alle misure di sicurezza adottate**;
- ottenere, nei casi previsti dall'articolo 17 del Regolamento (UE) 2016/679, la **cancellazione dei dati**, la **limitazione del trattamento**;
- **opporsi al trattamento**, nei casi e nei limiti previsti dall'articolo 21 del Regolamento (UE) 2016/679.

3. Le istanze per l'esercizio dei diritti sono presentate all'**esercente le funzioni di Titolare del trattamento** della struttura ovvero al **Designato competente**, ai recapiti istituzionali pubblicati sul sito internet dell'Amministrazione o della struttura interessata. In caso di richiesta di accesso alle immagini registrate mediante i sistemi di videosorveglianza, l'interessato è tenuto a fornire, per quanto possibile, elementi utili a consentire l'individuazione delle immagini che lo riguardano, indicando in particolare:

    - la **sede e il luogo** in cui si presume sia avvenuta la ripresa;
    - la **data e la fascia oraria** in cui l'evento si è verificato;
    - **elementi utili alla propria identificazione**, quali descrizione dell'abbigliamento, eventuali accessori indossati, presenza di accompagnatori o altre circostanze idonee a facilitare l'individuazione delle immagini.

Il Designato competente verifica l'eventuale esistenza delle immagini nei limiti del periodo di conservazione e comunica l'esito al richiedente. In caso positivo, la visione avviene con modalità idonee a tutelare i diritti di terzi eventualmente ripresi.

4. Qualora l'interessato richieda copia dei dati personali oggetto di trattamento, le immagini sono fornite in formato elettronico di uso comune, previo oscuramento dei dati riferiti ad altri soggetti eventualmente presenti, ai sensi dell'articolo 15, paragrafo 4, del Regolamento (UE) 2016/679.

5. I diritti possono essere esercitati anche da chi abbia un interesse proprio o agisca a tutela dell'interessato, nei limiti consentiti dalla normativa vigente. L'interessato può conferire delega o procura scritta a terzi per l'esercizio dei propri diritti.

6. In caso di mancato o insoddisfacente riscontro, l'interessato può proporre reclamo al Garante per la protezione dei dati personali, ai sensi dell'articolo 77 del Regolamento (UE) 2016/679, nonché avvalersi degli strumenti di tutela amministrativa e giurisdizionale previsti dagli articoli 78 e 79 del medesimo Regolamento e dalla normativa nazionale vigente.

7. In caso di richieste manifestamente infondate o eccessive, anche per il loro carattere ripetitivo, il Ministero può rifiutare di dare seguito alla richiesta ovvero addebitare un contributo spese ragionevole, ai sensi dell'articolo 12, paragrafo 5, del Regolamento (UE) 2016/679, fornendo adeguata motivazione.

## Articolo 13 – Norme di rinvio

1. Per quanto non espressamente disciplinato dal presente Regolamento, si applicano le disposizioni contenute nel Regolamento (UE) 2016/679, nel decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni e integrazioni, nonché le ulteriori disposizioni normative e regolamentari vigenti in materia di protezione dei dati personali.

2. Si rinvia altresì ai provvedimenti, alle linee guida e ai pareri dell'Autorità Garante per la protezione dei dati personali, nonché alla normativa nazionale ed europea in materia di videosorveglianza, sicurezza delle sedi istituzionali e tutela del patrimonio pubblico.
3. Restano ferme le disposizioni speciali applicabili alle amministrazioni pubbliche e quelle in materia di tutela dei lavoratori, con particolare riferimento all'articolo 4 della legge 20 maggio 1970, n. 300.