



“Consiglio regionale della Campania”

Servizio Sistemi Informativi

Determina N. 1407 del 24/11/2025

Oggetto: Adozione di “Disposizioni per la gestione del sistema di videosorveglianza”, in applicazione dei principi del RGPD.

Elenco firmatari

Francesco Crisci - Servizio Sistemi Informativi



Consiglio regionale della Campania

Servizio Sistemi Informativi

OGGETTO: Adozione di “Disposizioni per la gestione del sistema di videosorveglianza”, in applicazione dei principi del RGPD.

IL DIRIGENTE

Premesso che

- il Regolamento (UE) 2016/679, “*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)*” (di seguito RGPD), si applica al trattamento interamente o parzialmente automatizzato ovvero non automatizzato di dati personali (art. 2), effettuato da parte di un titolare del trattamento o di un responsabile che opera per conto di questo, nell’ambito delle rispettive attività (art. 3);
- le finalità ed i mezzi del trattamento di dati personali sono determinati dal titolare del trattamento; ed a questo spetta, tenuto conto della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento europeo (art. 24, co. 1); tali misure includono l’attuazione di politiche adeguate in materia di protezione dei dati (art. 24, co. 2);
- il responsabile incaricato di effettuare uno specifico trattamento per conto del titolare, tenendo conto della natura, dell’oggetto, del contesto e delle finalità del trattamento nonché della probabilità e gravità del rischio che questo può comportare per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato a tale rischio; le quali possono comprendere, fra l’altro, la capacità di assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (art. 32);
- con delibera dell’Ufficio di Presidenza n. 283 del 16 maggio 2025, i dirigenti *pro tempore* delle strutture amministrative dell’Ente (Direzioni, Settori, Servizi) sono stati individuati quali responsabili interni del trattamento, in ordine specificamente alle attività di trattamento dei dati afferenti ai processi di competenza di ciascuna struttura; ad essi, fra l’altro, è demandato di organizzare, gestire e vigilare tutte le operazioni di trattamento dei dati personali afferenti alle funzioni ed attività dell’ufficio dirigenziale ricoperto; attenersi alle misure tecniche ed organizzative adottate e collaborare alla loro predisposizione, aggiornamento o revisione; vigilare sulla corretta applicazione della regolamentazione interna adottata o da adottare a tutela



Consiglio regionale della Campania

della riservatezza nel trattamento dei dati;

Atteso che

- il Servizio Sistemi informativi è preposto alla gestione del sistema di videosorveglianza in esercizio presso il Consiglio regionale, tramite il quale viene effettuata la ripresa e registrazione di immagini riferibili alle persone fisiche in transito nello spazio monitorato; le quali sono perciò identificabili in base al loro aspetto o ad altri elementi visivi;
- la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini, nel caso di specie acquisite mediante dispositivi di video-ripresa, configura un trattamento di dati personali, in quanto tale soggetto all'applicazione dei principi del Regolamento (UE) 2016/679;
- il Garante per la Protezione dei Dati Personali, con Provvedimento dell' 8 aprile 2010, aveva già prescritto misure ed accorgimenti concernenti il trattamento di dati personali effettuato tramite sistemi di videosorveglianza, riguardo in specie alla necessità di informazione preventiva agli interessati e all'adozione di misure minime di sicurezza a protezione dei dati registrati, quali: l'individuazione delle responsabilità; la graduazione dei compiti e dei livelli di abilitazione; la limitazione delle operazioni e della conservazione; il Provvedimento, fra l'altro, ribadisce il divieto di controllo a distanza dell'attività lavorativa, volta a verificare, ad esempio, l'osservanza dei doveri di diligenza o la correttezza della prestazione lavorativa;
- le Linee-guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29/1/2020 dal Comitato europeo per la Protezione dei Dati, forniscono ulteriori indicazioni sull'applicazione della normativa del Regolamento generale, riguardo in specie alla liceità e necessità del trattamento; alla comunicazione delle immagini a terzi, in particolare alle autorità di polizia; ai diritti dell'interessato, in particolare di accesso e di cancellazione; agli obblighi informativi sia preventivi (Informativa minima) che secondari (Informativa completa); alle misure tecniche ed organizzative da prendere in considerazione nell'elaborazione delle politiche e procedure di videosorveglianza, al fine di garantire l'adeguata sicurezza del sistema e dei dati;
- in ragione dell'art. 17 del decreto legislativo 7 marzo 2005 n. 82 "*Codice dell'amministrazione digitale*", il quale attribuisce al Responsabile della Transizione al Digitale, fra l'altro, i compiti di: indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture (lett. c) e di analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione (lett. e), il RTD ha espresso indicazioni riguardo alla necessità di adeguare il sistema di videosorveglianza a criteri di sicurezza informatica, anche in ottica di salvaguardia della riservatezza dei dati durante la conservazione, la trasmissione ed il trattamento, in linea con le misure utilizzate a protezione dei sistemi informatici in uso nell'Amministrazione;
- pertanto, la gestione del sistema di videosorveglianza ed il trattamento di dati che ne comporta devono essere effettuati in conformità alla normativa vigente in materia, tenendo conto degli indirizzi applicativi a riguardo assunti sia a livello nazionale che europeo;



Consiglio regionale della Campania

Dato atto che

- il Servizio Sistemi informativi, in raccordo, per quanto di spettanza, con l'Ufficio Prevenzione della Corruzione, Trasparenza, Privacy e con l'Ufficio Transizione al Digitale, ha elaborato e predisposto il documento allegato, recante *“Disposizioni per la gestione del sistema di videosorveglianza”*, nonché l'*Informativa* generale, ai sensi dell'art. 13 del RGPD, riguardante il trattamento dei dati identificativi raccolti e registrati;
- il documento contiene le disposizioni volte a garantire che la configurazione del sistema di videosorveglianza attivato presso il Consiglio regionale e la sua gestione nonché il trattamento di dati personali che ne consegue si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, in conformità alla normativa vigente in materia e ai pertinenti indirizzi delle Autorità competenti;
- in particolare, le *Disposizioni* riguardano:
 - le modalità di acquisizione e le tipologie di trattamento cui le immagini possono essere sottoposte secondo i principi di liceità, di limitazione delle finalità e di necessità e proporzionalità;
 - le regole di condotta cui il personale autorizzato ovvero gli addetti alla vigilanza devono attenersi nell'esercizio delle mansioni o compiti di cui sono incaricati;
 - i criteri di sicurezza, sia fisica che informatica, applicati al sistema di videosorveglianza;
 - le garanzie per l'esercizio dei diritti riconosciuti agli interessati, dal Regolamento generale o dalla legislazione nazionale;
- ai fini dell'esecuzione delle attività di videosorveglianza, – tenuto conto delle *“Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del Regolamento (UE) 2016/679”* del Gruppo di Lavoro Articolo 29 del 4/4/2017 ed il Provvedimento dell'Autorità Garante dell' 11/10/2018 *“Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679”* – il Servizio Sistemi informativi ha altresì adempiuto alla valutazione preliminare d'impatto sulla protezione dei dati, ai sensi dell' art. 35 del RGPD; in ordine alla quale il Responsabile della Protezione dei Dati ha espresso parere favorevole all'implementazione del trattamento;

Considerato, dunque, che

- le *“Disposizioni per la gestione del sistema di videosorveglianza”* costituiscono misura organizzativa adeguata ad assicurare la conformità dei trattamenti effettuati tramite la videoregistrazione delle immagini, ed a seguito o in dipendenza di questa, alla normativa europea e nazionale, in ragione dei principi di responsabilizzazione (artt. 24 e 25, RGPD) e di sicurezza del trattamento (art. 32, RGPD), recependo peraltro gli indirizzi espressi sia dall'Autorità garante nazionale (Provvedimento GPDP in materia di videosorveglianza dell'8



Consiglio regionale della Campania

aprile 2010) sia dal Comitato europeo per la protezione dei dati (Linee-guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video);

Ritenuto

- di adottare le allegate “*Disposizioni per la gestione del sistema di videosorveglianza*” (All. A), predisposte a cura del Servizio Sistemi informativi, dell’ Ufficio Transizione al Digitale e dell’ Ufficio P.C.T.Privacy, nonché di prendere atto dell’ *Informativa* in forma estesa (All. B), redatta ai sensi dell’ art. 13 del RGPD, in relazione allo specifico trattamento, e della Valutazione d’Impatto (All. C), preliminare al trattamento, ai sensi dell’art. 35 del RGPD;

Visti

- il Regolamento del 27/6/2023 “*Ordinamento amministrativo del Consiglio regionale*”;
- il Regolamento (UE) 2016/679, “*Regolamento generale sulla protezione dei dati*”;
- il d.lgs. 30 giugno 2003 n. 196, “*Codice in materia di protezione dei dati personali*”;
- il Provvedimento GPDP in materia di videosorveglianza dell’8 aprile 2010;
- le Linee-guida CEPD n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video;
- la delibera dell’Ufficio di Presidenza n. 283 del 16 maggio 2025;

determina

- di adottare, quale misura organizzativa adeguata, l’allegato documento “*Disposizioni per la gestione del sistema di videosorveglianza*” (All. A), costituente parte integrante e sostanziale del presente atto;
- di prendere atto dell’*Informativa* redatta, in relazione allo specifico trattamento, ai sensi dell’art. 13 del Regolamento (UE) 2016/679 (All. B); l’*Informativa* è resa disponibile tramite il sito istituzionale;
- di prendere atto, ai fini dell’esecuzione del trattamento, della Valutazione d’Impatto (All. C), svolta ai sensi dell’art. 35 del Regolamento (UE) 2016/679 dal Servizio Sistemi informativi, e del parere favorevole espresso dal Responsabile della Protezione dei Dati;
- di precisare che i dirigenti *p.t* delle strutture amministrative competenti individuano il personale interno autorizzato al trattamento nonché adottano le direttive o istruzioni idonee per la messa in conformità del sistema di videosorveglianza in essere;
- di precisare altresì che, a seguito dell’approvazione, le *Disposizioni* sono notificate, a cura della struttura competente alla gestione dei servizi di vigilanza, alla ditta affidataria, la quale è tenuta, in esecuzione del contratto di servizio, ad indicare gli addetti da autorizzare ed abilitare alla



Consiglio regionale della Campania

videosorveglianza;

- di trasmettere il presente atto al Direttore della Direzione Risorse umane, finanziarie e strumentali, al Segretario generale, al Servizio Sistemi informativi, all'ufficio p.c.t. privacy, all'ufficio transizione al digitale.

IL DIRIGENTE

Francesco Crisci



DISPOSIZIONI ORGANIZZATIVE PER LA GESTIONE DEL SISTEMA DI VIDEOSORVEGLIANZA

- 1. Finalità**
- 2. Definizioni**
- 3. Principi del trattamento**
- 4. Valutazione d'impatto sulla protezione dei dati**
- 5. Informazione agli interessati**
- 6. Titolare e responsabile del trattamento**
- 7. Autorizzati al trattamento**
- 8. Caratteristiche tecniche del sistema di videosorveglianza**
- 9. Modalità di raccolta e trattamento dei dati**
- 10. Sicurezza dei dati**
- 11. Accesso ai dati**
- 12. Diritti dell'interessato.**
- 13. Pubblicazione e comunicazione.**

1. Finalità

Le presenti *Disposizioni* sono adottate al fine di garantire che il trattamento dei dati personali, effettuato mediante il sistema di videosorveglianza attivato presso il Consiglio regionale della Campania, si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, in conformità alla normativa vigente in materia e ai pertinenti indirizzi delle Autorità competenti, specificatamente:

- Regolamento (UE) 2016/679 “*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)*” (di seguito RGPD);

- Decreto legislativo 30 giugno 2003 n. 196 “*Codice in materia di protezione dei dati personali*”;
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di videosorveglianza dell’8 aprile 2010;
- Linee-guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate dal Comitato europeo per la Protezione dei Dati.

Il sistema di videosorveglianza è attivato in particolare per i seguenti scopi:

- la sicurezza della sede ove si espletano le attività istituzionali ed amministrative del Consiglio (edificio F13 del Centro direzionale di Napoli);
- la salvaguardia dei beni immobili e mobili nella disponibilità dell’Amministrazione, anche al fine di prevenire atti di vandalismo o danneggiamenti;
- la prevenzione di eventi rischiosi per la sicurezza dei luoghi sottoposti a sorveglianza;
- l’acquisizione di elementi probatori nel caso di verifica di illeciti penali.

In virtù dell’art. 4 dello Statuto dei lavoratori (Legge 20 maggio 1970, n. 300), l’impianto di videosorveglianza non potrà essere utilizzato, in alcun modo, per effettuare controlli diretti e/o a distanza sull’attività lavorativa dei dipendenti del Consiglio regionale o di altri soggetti che operano, a vario titolo, nel contesto organizzativo del Consiglio.

2. Definizioni

Per chiarezza espositiva, si richiamano le definizioni del Regolamento generale sulla protezione dei dati, rilevanti ai fini ed in relazione all’oggetto delle presenti *Disposizioni*:

- «*dato personale*», qualsiasi informazione riguardante una persona fisica identificata o identificabile («*interessato*»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; dunque, le immagini o sequenze di immagini raccolte tramite strumenti di video-ripresa costituiscono dati personali idonei ad identificare, in base all’aspetto o altri elementi specifici, le persone che rientrano nello spazio monitorato;
- «*trattamento*», qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione; dunque, l’attività di video-ripresa e video-registrazione nonché la visione, in diretta o differita, delle immagini, la loro duplicazione per la trasmissione a terzi ove necessaria e legittima, la periodica cancellazione costituiscono trattamenti di dati personali, da eseguire in conformità della normativa generale, sopra richiamata;
- «*archivio*», qualsiasi insieme strutturato di dati personali accessibile secondo criteri determinati; dunque, il complesso delle immagini o sequenze di immagini raccolte tramite le apparecchiature

di video-ripresa e registrazione costituisce un archivio di dati personali, relativi ai soggetti che transitano nelle aree sottoposte a sorveglianza;

- «*titolare del trattamento*», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- «*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;
- «*destinatario*», la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi; le video-registrazioni trattate dal Consiglio regionale possono essere oggetto di comunicazione esclusivamente all'autorità giudiziaria o alle forze di polizia; l'accesso è consentito all'interessato o al terzo legittimato; ne è esclusa in ogni modo la diffusione;
- «*terzo*», la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento o la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- «*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.

3. Principi del trattamento

Al trattamento operato tramite il sistema di videosorveglianza si applicano i principi dell'art. 5 del RGPD, come di seguito specificati:

principio di liceità: il trattamento avviene per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, paragrafo 1, lett. e) del RGPD), ossia la sicurezza della sede istituzionale ove si svolgono gli uffici legislativi ed amministrativi nonché per il perseguimento del legittimo interesse (art. 6, paragrafo 1, lett. f) del RGPD) alla salvaguardia dei beni dell'Amministrazione, anche a scopo preventivo; pertanto, i trattamenti di videosorveglianza, nell'ambito definito con le presenti *Disposizioni*, non necessitano dell'acquisizione del consenso espresso da parte dei potenziali interessati;

principio di limitazione delle finalità: i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità (art. 5, paragrafo 1, lett. b) del RGPD); la videosorveglianza è istituita come misura di sicurezza complementare all'ordinaria attività di vigilanza;

principio di necessità: in applicazione dei criteri di pertinenza, adeguatezza e limitazione dei dati (art. 5, paragrafo 1, lett. c), del RGPD), il sistema di videosorveglianza ed annessi sistemi informativi sono configurati in modo da ridurre al minimo l'acquisizione di dati personali e identificativi o da escluderne il trattamento quando le finalità perseguite possono essere realizzate mediante dati anonimi, consentendo di identificare l'interessato solo in caso di necessità. Pertanto, il sistema di videosorveglianza in esercizio esclude riprese superflue, eccessive o ridondanti; qualora non sia necessario individuare le persone, il sistema dev'essere configurato, per impostazione di base, in modo da poter impiegare solo dati anonimi con riprese d'insieme ed il

software utilizzato dev'essere preventivamente impostato per cancellare periodicamente ed automaticamente i dati registrati.

principio di proporzionalità: la raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. Pertanto, la necessità di impiego del sistema di videosorveglianza dev'essere commisurata al grado di rischio concreto, escludendo la rilevazione su aree, ambienti o transiti in relazione ai quali non sia ravvisabile una concreta esposizione ad eventi di pericolo e, dunque, un'esigenza di controllo, anche a scopo di deterrenza. L'impianto di videosorveglianza coadiuva l'attività di controllo, finalizzata alla sicurezza dei luoghi e alla protezione di beni, svolta da parte degli addetti alla vigilanza; l'utilizzo delle apparecchiature di ripresa è limitato alle aree interne o esterne di esclusiva pertinenza dell'Ente ritenute sensibili e all'angolo di visuale adeguato alla raccolta / registrazione delle sole immagini indispensabili agli scopi di protezione anzidetti, evitando modalità di ripresa non pertinenti o eccedenti.

4. Valutazione di impatto sulla protezione dei dati

Viste le *“Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del Regolamento (UE) 2016/679”* del Gruppo di Lavoro Articolo 29 del 4/4/2017 ed il Provvedimento dell'Autorità Garante dell'11/10/2018 *“Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679”*, il trattamento effettuato mediante il sistema di videosorveglianza è sottoposto a previa Valutazione d'Impatto sulla protezione dei dati, ai sensi dell'art. 35 del RGPD, redatta a cura della struttura competente alla gestione del sistema di videosorveglianza.

La Valutazione è soggetta a periodica revisione, al fine di verificarne l'adeguatezza anche in caso di adozione di nuove soluzioni tecnologiche o organizzative.

5. Informazione agli interessati

Il titolare e il responsabile del trattamento adottano metodi comunicativi adeguati, in modo da preavvisare gli interessati della possibile esposizione a videoregistrazione ed in modo da mettere a loro disposizione un'informazione completa sulle modalità del trattamento in atto; si osservano le prescrizioni dettate dal Provvedimento del Garante e dalle Linee-guida del CEPD.

In particolare, le persone fisiche che accedono all'area sottoposta a videosorveglianza devono essere informate mediante apposita segnaletica di avvertimento, collocata in posizione chiaramente visibile e prima del raggio d'azione della videoripresa. I cartelli segnaletici contengono l'Informativa “minima” indicante il titolare del trattamento e la finalità perseguita.

L'Informativa dettagliata, contenente gli elementi di cui all'art. 13 del RGPD, è redatta e, all'occorrenza, aggiornata dalla struttura responsabile del trattamento ed è resa disponibile tramite il sito istituzionale dell'Ente.

6. Titolare e Responsabile del trattamento

Il Titolare del trattamento dei dati è il Consiglio regionale della Campania.

Il Responsabile interno del trattamento è individuato nel dirigente della struttura competente alla gestione del sistema di videosorveglianza.

Il Responsabile interno assicura che le attività di trattamento siano conformi alle disposizioni di legge vigenti, alle prescrizioni dell'Autorità garante, alla regolamentazione adottata dall'Ente, incluse le presenti *Disposizioni*, alle istruzioni fornite dal Titolare nell'atto di designazione.

In particolare, il Responsabile del trattamento:

- controlla che il trattamento effettuato mediante il sistema di videosorveglianza avvenga nel rispetto dei principi di cui all'art. 5 del RGPD, ossia assicura che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo lecito, corretto e trasparente e non incompatibile con tali finalità;
- adotta o, se del caso, propone l'adozione delle misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del RGPD, e controlla l'attuazione di tali misure da parte degli addetti ed autorizzati al trattamento;
- provvede ad istruire gli autorizzati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati;
- assicura che gli autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle stesse finalità;
- emana disposizioni con cui impartisce direttive o istruzioni operative, rivolte al personale autorizzato, agli addetti alla vigilanza o alla assistenza tecnica, e vigila sulla loro osservanza e sul rispetto degli obblighi di corretta e lecita acquisizione dei dati ed utilizzazione degli stessi.

Il Responsabile del trattamento è autorizzato a designare altro responsabile, esterno all'Amministrazione, qualora sia necessario per ragioni organizzative di esercizio o di assistenza del sistema di videosorveglianza. In tal caso, il trattamento demandato al responsabile esterno è disciplinato dal contratto di servizio stipulato ai sensi dell'art. 28, paragrafi 3 e 4, del RGPD, alle cui prescrizioni di dettaglio integralmente si rinvia.

7. Autorizzati al trattamento

Il Responsabile del trattamento individua, nell'ambito della struttura organizzativa, i soggetti autorizzati al trattamento ai sensi dell'art. 2-*quaterdecies* del d.lgs. n. 196/2003, in quanto incaricati di specifici compiti e funzioni connessi alla videosorveglianza (ad esempio, utilizzazione degli impianti, visione o gestione delle registrazioni, custodia ed accesso alla sala operativa, etc.).

L'individuazione è effettuata mediante disposizione di servizio, la quale contenga la chiara e puntuale definizione dell'ambito del trattamento consentito, la specificazione delle operazioni cui l'incaricato è abilitato, le istruzioni sulla corretta gestione dei sistemi e sull'utilizzo delle apparecchiature installate, le informazioni sull'osservanza della normativa di riferimento e delle presenti *Disposizioni*.

Le credenziali abilitanti sono rilasciate, su richiesta del dirigente *p.t.* responsabile, al personale interno o agli addetti alla vigilanza, di volta in volta indicati, in relazione ai compiti assegnati ed autorizzati.

In particolare, il soggetto autorizzato:

- accede ai sistemi utilizzando esclusivamente le proprie credenziali ed evita, in caso di allontanamento anche temporaneo, che terzi possano accedere alla sessione in corso, avendo cura di disconnettere l'utenza;
- adopera ogni cautela a salvaguardia della massima riservatezza dei dati di cui abbia conoscenza o disponibilità a motivo dello svolgimento delle proprie mansioni;
- osserva scrupolosamente le direttive e le istruzioni operative impartite dal Responsabile del trattamento all'atto della preposizione al trattamento o con successive disposizioni e si attiene doverosamente alle misure di sicurezza predisposte dall'Amministrazione;
- si astiene da qualunque utilizzo non autorizzato, improprio o illecito dei dati personali (ad esempio, duplicazione, manipolazione, divulgazione non consentita, etc.);
- fornisce, al Responsabile del trattamento e al Responsabile della Protezione dei Dati, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

8. Caratteristiche del sistema di videosorveglianza

Il sistema di videosorveglianza in esercizio presso il Consiglio regionale è strutturato in modo da svolgere le funzionalità di ripresa delle immagini (tramite telecamere fisse posizionate nelle aree sensibili), di visione in diretta o differita e di registrazione e conservazione (tramite apparecchiature collocate in apposito locale). La sala operativa è accessibile soltanto agli incaricati della vigilanza e al personale specificamente autorizzato.

Il sistema di videosorveglianza non opera in modalità integrata con sistemi o servizi di altri soggetti pubblici o privati. Le immagini riprese vengono messe a disposizione esclusivamente dei soggetti legittimati (ad esempio, forze dell'ordine, interessati, etc.), che ne facciano richiesta come indicato nel *paragrafo 11*.

9. Modalità di raccolta e trattamento dei dati

I trattamenti di dati personali nell'ambito dell'attività di videosorveglianza avvengono in maniera conforme alla normativa vigente, al Provvedimento del Garante per la Protezione dei Dati Personali in materia di videosorveglianza dell'8 aprile 2010, nonché alle Linee-guida n. 3/2019 del Comitato Europeo per la Protezione dei Dati sul trattamento dei dati personali attraverso dispositivi video.

Al fine di limitare l'attività di videosorveglianza all'acquisizione delle immagini indispensabili agli scopi di vigilanza, secondo criteri di necessità proporzionalità e non eccedenza, le riprese riguardano esclusivamente spazi e beni, di pertinenza dell'Amministrazione (edificio della sede istituzionale del Consiglio), individuati come sensibili (ad esempio, ingressi, aree di transito, locali di non frequente accesso o dove sono presenti impianti tecnologici, etc.); pertanto, le telecamere sono posizionate ed orientate in modo da escludere dal campo visuale i luoghi circostanti e da evitare videoregistrazioni indiscriminate di persone o cose o con un livello di dettaglio non funzionale alle finalità del sistema.

Le immagini raccolte tramite il sistema di videosorveglianza sono conservate per un periodo massimo di n. 7 giorni dalla rilevazione. Soltanto in caso di richiesta dell'Autorità giudiziaria o delle Forze di

polizia, motivata in base ad esigenze investigative o di giustizia, la conservazione potrebbe avere durata superiore, in ragione della necessità di aderire, per il tempo occorrente, all'ordine di custodia o consegna di copia delle registrazioni.

Il sistema è programmato in modo da operare, alla scadenza del periodo di conservazione, la cancellazione automatica e definitiva delle registrazioni acquisite.

10. Sicurezza dei dati

I dati trattati mediante il sistema di videosorveglianza (ossia le registrazioni digitali delle sequenze di video-ripresa) sono protetti, tanto nella fase di raccolta che di conservazione, con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato ai possibili rischi di perdita o alterazione, di accesso accidentale o illegale, di eventuale conseguente divulgazione non autorizzata.

Dette misure, in particolare, assicurano la riservatezza, l'integrità, la disponibilità dei dati e del sistema di trattamento, includendo azioni di ripristino in caso di incidente e di controllo degli accessi e dell'operatività di sistema; le stesse sono soggette a periodica verifica di efficacia.

A questo fine, sono adottate le seguenti specifiche misure organizzative e tecniche:

- a) i soggetti responsabili e autorizzati al trattamento sono in possesso di credenziali di autenticazione con abilitazioni gestionali diversificate, in base ai compiti attribuiti a ciascuno, in modo da permettere di effettuare soltanto le operazioni di rispettiva competenza;
- b) la visione delle immagini in sincronia con la ripresa è operata esclusivamente dai soggetti specificamente autorizzati (personale interno e addetti di vigilanza); i soggetti abilitati a visionare le immagini, in diretta o in differita, non hanno la possibilità di effettuare contestualmente operazioni di cancellazione o di duplicazione;
- c) i soggetti abilitati alla visione, in diretta o differita, delle immagini adottano le cautele necessarie ad impedire che terzi non autorizzati possano accedere al sistema; ad esempio, evitando di lasciare le postazioni prive di sorveglianza e chiudendo o sospendendo le sessioni in corso in caso di allontanamento;
- d) la cancellazione al termine del periodo di conservazione avviene in maniera automatica ed irreversibile; in caso di richiesta di accesso, da parte di soggetti legittimati, al materiale visivo ancora in corso di trattamento, il responsabile del trattamento autorizza la duplicazione ed il salvataggio per la successiva messa a disposizione;
- e) il sistema di videosorveglianza in esercizio è configurato, per impostazione di base, in modo da minimizzare il trattamento delle immagini, consentendo di identificare l'interessato solo in caso di necessità ed escludendo l'identificazione di terzi mediante offuscamento delle immagini;
- f) gli apparati di conservazione delle riprese digitali sono protetti dal rischio di manomissione o di utilizzo abusivo, in quanto posizionati all'interno di locali ad accesso riservato; soltanto i soggetti autorizzati possono utilizzare le postazioni di controllo, per effettuare, nei casi in cui sia indispensabile per gli scopi perseguiti, operazioni di trattamento delle immagini;
- g) la trasmissione tramite la rete locale delle immagini riprese dagli apparati di videosorveglianza avviene previa applicazione di tecniche crittografiche che ne garantiscono la riservatezza;

- h) ove siano necessari interventi di manutenzione del sistema, i soggetti incaricati possono accedere alle videoregistrazioni soltanto se ciò sia indispensabile per esigenze tecniche; le operazioni manutentive e le verifiche avvengono in presenza del personale abilitato alla visione delle immagini.

11. Accesso ai dati

L'accesso alle videoregistrazioni, nel periodo prestabilito della loro conservazione, è consentito esclusivamente ai seguenti soggetti:

- a) il Responsabile del trattamento nonché i soggetti previamente autorizzati, in base alle condizioni e modalità previste nell'atto autorizzativo, in caso di effettiva necessità per dare attuazione agli scopi previsti o per dare seguito alla richiesta di altre autorità o terzi legittimati;
- b) le Forze di Polizia e l'Autorità giudiziaria, sulla base di espressa richiesta dell'organo competente, acquisita dall'Amministrazione;
- c) l'interessato al trattamento (ad esempio, la persona che figura nella videoregistrazione), sulla base di richiesta scritta formulata ai sensi dell'art. 15 del RGPD e secondo le modalità di cui al *paragrafo* successivo;
- d) i soggetti aventi diritto all'accesso ai sensi degli artt. 22 e seguenti della legge n. 241/1990, secondo le condizioni di legge previste, qualora sia necessario per curare o per difendere interessi giuridici del richiedente prevalenti rispetto agli opposti interessi di sicurezza o riservatezza. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

12. Diritti dell'interessato

Ad ogni interessato è garantito l'esercizio dei diritti previsti dagli artt. 15-22 del RGPD, sulla base di specifica istanza, presentata nei modi comunicati con l'Informativa sul trattamento.

Nel caso di richiesta di accesso alle videoregistrazioni, l'interessato dovrà indicare: le circostanze di luogo e temporali della possibile ripresa; gli elementi di riconoscimento (ad esempio, abbigliamento o accessori, la dinamica in atto); l'eventuale presenza di altre persone (ad esempio, accompagnatori).

Il Responsabile del trattamento e/o il soggetto autorizzato accertano l'effettiva esistenza delle videoregistrazioni e ne danno comunicazione al richiedente, fissando il giorno, l'ora ed il luogo in cui il medesimo potrà prendere visione delle immagini che lo riguardano; ovvero, qualora questi, ai sensi dell'art. 15, paragrafo 3, del RGPD, abbia chiesto di ottenere copia delle videoregistrazioni, si procederà al rilascio delle immagini in un formato elettronico di uso comune, previo oscuramento degli elementi identificativi non pertinenti o riferiti ad altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio all'art. 15, paragrafo 4, del RGPD.

Ai sensi dell'art. 13, paragrafo 2, lett. d) e dell'art. 77 del RGPD, l'interessato ha diritto di proporre reclamo motivato al Garante per la Protezione dei Dati personali, se ritiene che il trattamento dei dati che lo riguardano non è conforme al Regolamento ovvero se la risposta ad un'istanza per l'esercizio dei diritti a lui spettanti non è tempestiva o soddisfacente.

Resta ferma l'esperibilità degli strumenti di tutela amministrativa o giurisdizionale come previsto dagli artt. 78-79 del RGPD nonché la risarcibilità del danno materiale o immateriale a norma dell'art. 82 del RGPD.

13. Pubblicazione e revisioni

Il presente atto è pubblicato, per la consultazione, sul portale interno dell'Ente; ed è soggetto a periodica verifica di adeguatezza, anche su indicazione del Responsabile della Protezione dei Dati, ove designato, in caso di mutamenti del quadro normativo o di successivi indirizzi dell'Autorità garante o di adeguamenti ed innovazioni tecnologiche del sistema.



VIDEOSORVEGLIANZA

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

La presente *Informativa* riguarda le finalità e le modalità del trattamento dei dati identificativi acquisiti tramite il sistema di videosorveglianza installato ed in esercizio presso la sede istituzionale del Consiglio regionale (edificio F13, Centro direzionale di Napoli).

La presenza dell'impianto di videoripresa è segnalata da idonei cartelli con relativa informativa minima, collocati prima del raggio di azione delle telecamere o nelle loro immediate vicinanze.

Le immagini videoregistrate costituiscono dati personali ed in quanto tali sono soggette alla disciplina del Regolamento (UE) 2016/679, *“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)”*.

Titolare del trattamento dei dati (e responsabile del trattamento).

Il Titolare del trattamento è il Consiglio regionale della Campania.

Indirizzo: Centro Direzionale, Isola F13 - 84013 Napoli.

p.e.o.: protocollo@cr.campania.it; p.e.c.: protocollo.generale@pec.cr.campania.it

Il Responsabile del trattamento è il dirigente p.t. del Servizio Sistemi Informativi.

Indirizzo: Centro Direzionale, Isola F13 - 84013 Napoli.

p.e.o.: servizio.si@cr.campania.it; p.e.c.: protocollo.generale@pec.cr.campania.it

Responsabile della protezione dei dati

Il Responsabile della protezione dei dati, cui gli interessati possono rivolgersi per le questioni relative al trattamento, può essere contattato ai seguenti recapiti:

Indirizzo: Centro Direzionale, Isola F13 - 84013 Napoli.

p.e.o.: dpo@cr.campania.it; p.e.c.: protocollo.generale@pec.cr.campania.it

Finalità del trattamento dei dati personali

L'acquisizione delle immagini tramite il sistema di videosorveglianza è operata per le seguenti finalità:

- la sicurezza della sede ove si espletano le attività istituzionali ed amministrative del Consiglio (edificio F13 del Centro direzionale di Napoli);
- la salvaguardia dei beni immobili e mobili nella disponibilità dell'Amministrazione, anche al fine di prevenire atti di vandalismo o danneggiamenti;
- la prevenzione di eventi rischiosi per la sicurezza dei luoghi sottoposti a sorveglianza;
- l'acquisizione di elementi probatori nel caso di verifica di illeciti penali.

Base giuridica del trattamento

Il trattamento dei dati avviene, senza che sia necessario acquisire il previo consenso espresso dell'interessato, sulla base dell'art. 6, par. 1, lett. e) dal RGPD e dell'art. 2-ter del d.lgs. n. 196/2003, *«per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri»* nonché, sulla base della lett. f) del citato art. 6, *«per il perseguimento del legittimo interesse del titolare»*.

Modalità del trattamento

Il trattamento avviene tramite sistemi digitali di acquisizione e memorizzazione delle immagini, sotto il controllo di personale appositamente formato e autorizzato, nel rispetto dei principi di necessità,

proporzionalità e non eccedenza e di riservatezza e sicurezza, in conformità alla normativa generale (RGPD e Codice della privacy) e alle linee-guida sulla videosorveglianza dell'Autorità garante e del Comitato europeo per la protezione dei dati personali.

Il trattamento di videoripresa è limitato alle aree interessate dall'esigenza di prevenzione del rischio; le procedure di acquisizione e conservazione sono integrate con idonee misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato ai possibili rischi di perdita o alterazione, di accesso accidentale o illegale, di eventuale conseguente divulgazione non autorizzata.

L'accesso alle immagini, in diretta o in differita, è consentito esclusivamente al personale autorizzato.

Destinatari (o categorie di destinatari) di dati personali

In relazione alle finalità del trattamento, le videoregistrazioni possono essere messe a disposizione dell'Autorità giudiziaria o delle Forze di Polizia, su specifica richiesta motivata in base ad esigenze investigative o di giustizia; ovvero comunicate a soggetti terzi ove legittimati, in base a disposizioni di legge, all'accesso, che sarà consentito mediante l'utilizzo di tecniche di oscuramento dei dati non strettamente indispensabili.

Periodo di conservazione e durata del trattamento

Le immagini acquisite tramite il sistema di videosorveglianza sono conservate per un periodo di n. 7 giorni. Soltanto in caso di richiesta dell'Autorità giudiziaria o delle Forze di polizia, motivata in base ad esigenze investigative o di giustizia, la conservazione potrebbe avere durata superiore, in ragione della necessità di aderire, per il tempo occorrente, all'ordine di custodia o consegna di copia delle registrazioni.

Diritti dell'interessato

L'interessato può esercitare, mediante richiesta al Titolare del trattamento ovvero al Responsabile della protezione dei dati indirizzata ai rispettivi recapiti, i diritti previsti dagli articoli da 15 a 22 del RGPD:

- **diritto di accesso, art. 15.** *L'interessato ha diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati e alle altre informazioni sul trattamento.*
- **diritto di rettifica, art. 16.** *L'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo nonché di ottenere l'integrazione dei dati personali incompleti.*
- **diritto alla cancellazione, art. 17.** *L'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo.*
- **diritto di limitazione del trattamento, art. 18.** *L'interessato ha il diritto di ottenere la limitazione del trattamento, nelle ipotesi di contestazione dell'esattezza dei dati, di illiceità del trattamento, di utilizzo per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, di opposizione per motivi legittimi.*
- **obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento, art. 19.** *L'interessato ha diritto ad ottenere che il titolare del trattamento comunichi a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento.*
- **diritto alla portabilità dei dati, art. 20.** *L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e ha il diritto ad ottenere che i dati siano trasmessi ad altro titolare del trattamento senza impedimenti, qualora il trattamento si basi sul consenso o su un contratto e qualora il trattamento sia effettuato con mezzi automatizzati.*
- **diritto di opposizione, art. 21.** *L'interessato ha diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento di dati personali che lo riguardano.*

Diritto di proporre reclamo

Ai sensi dell'art. 13, par. 2, lett. d), e dell'art. 77 del RGPD, l'interessato può proporre reclamo motivato al Garante per la Protezione dei Dati Personali, qualora ritenga che il trattamento dei dati che lo riguardano non sia conforme alla normativa applicabile. Le informazioni sulle modalità di presentazione possono essere

consultate sul sito istituzionale dell'Autorità, www.garanteprivacy.it