

Regolamento Videosorveglianza INDIRE

(approvato con deliberazione del CDA n. 75 del 27.06.2024)

(aggiornamento approvato con deliberazione del CDA n. 63 del 29.10.25)

Premessa

INDIRE, avendo riguardo all'ubicazione e alle caratteristiche strutturali degli immobili e dei locali all'interno dei quali svolge le proprie attività istituzionali di interesse pubblico, nell'intento di voler garantire una maggiore attenzione alla tutela del proprio patrimonio e alla sicurezza, si è dotata, nel rispetto dei principi di liceità, correttezza e trasparenza, minimizzazione, integrità e riservatezza, limitazione della conservazione e della finalità, di un sistema di videosorveglianza installato presso:

- la sede di Firenze sita in Via Cesare Lombroso 6/15 dove è sita l'Agenzia Nazionale Erasmus+, il settore ricerca dell'ente e dove è presente una sala CED;
- la sede centrale di Firenze, c/o Palazzo Gerini, sita in Via M. Buonarroti 10 dove risiedono la Presidenza, la Direzione Generale, e il Consiglio di amministrazione dell'Istituto, oltre agli uffici amministrativi e finanziari, alle aree di ricerca e ai sistemi informativi;
- la sede del Nucleo Territoriale Sud di INDIRE ed Erasmus+ sita in via Melisurgo 4 Napoli.

Il presente Regolamento disciplina il funzionamento dei sistemi di videosorveglianza attualmente installati presso le suddette sedi di Firenze e di Napoli e di eventuali ulteriori impianti che potranno essere attivati in futuro dall'Istituto nonché il trattamento dei dati personali effettuato tramite le telecamere di sorveglianza.

Per quanto non espressamente previsto dal presente Regolamento, si rinvia integralmente alle norme in materia di tutela dei dati personali: Regolamento (UE) 2016/679; D. Lgs. n. 196/2003; Provvedimento in materia di videosorveglianza 8 aprile 2010 (per quanto applicabile) dell'Autorità Garante per la protezione dei dati personali; Linee guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate il 29 gennaio 2020 dall'*European Data Protection Board* ("**Linee Guida EDPB**"); Legge n. 300/1970 e successive modifiche e integrazioni.

Articolo 1 – Definizioni

- **"GDPR"**: 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);
- **"Codice privacy"**: decreto legislativo 30 giugno 2003 n. 196/2003 "Codice in materia di protezione dei dati personali" recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679;
- **"Garante"**: Garante per la protezione dei dati personali di cui agli articoli 153 e ss. del Codice privacy;
- **"Provvedimento Generale"**: Provvedimento in materia di videosorveglianza emanato dal Garante in data 08.04.2010;
- **"DPO" o "RPD"**: il Responsabile della protezione dei dati di INDIRE;
- **"dato personale"**: qualunque informazione relativa a persona fisica identificata o identificabile; 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **"trattamento"**: qualunque operazione o complesso di operazioni, compiute con o senza l'ausilio di processi informatizzati 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, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione e la distruzione;
- **"Titolare"** del trattamento: la persona fisica o giuridica, 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;
- **"Referente Privacy"**: la persona fisica che, espressamente designata dal Titolare

nell'ambito del proprio assetto organizzativo e organigramma privacy, opera sotto la sua autorità con compiti di supervisione e funzioni connesse al trattamento delle immagini/videoregistrazioni;

- **"Autorizzato"**, la persona fisica formalmente autorizzata dal Titolare a compiere operazioni di trattamento sulle immagini/videoregistrazioni;
- **"Interessato"**: la persona fisica identificata o identificabile attraverso i dati personali;
- **"Comunicazione"**: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dalle persone autorizzate ai sensi dell'art. 2-quaterdecies del Codice Privacy, in qualunque forma, anche mediante la loro messa a disposizione o consultazione o mediante interconnessione;
- **"Diffusione"**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **"Dato anonimo"**: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

Articolo 2 - Principi generali

1. La raccolta, la rilevazione, l'accesso, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configurano un trattamento di dati personali.
2. Il trattamento di dati personali attraverso sistemi di videosorveglianza da parte di INDIRE avviene esclusivamente nell'ambito delle finalità di cui al successivo articolo 3 del presente regolamento.
3. La determinazione dell'ubicazione delle videocamere e delle modalità di ripresa e il trattamento dei dati raccolti vengono effettuati, *inter alia*, in osservanza dei seguenti principi:
 - rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, con particolare riferimento alla riservatezza e alla identità e alle abitudini personali;
 - **principio di liceità**: il trattamento dei dati è circoscritto alle attività connesse all'esercizio di pubblici poteri e di interesse pubblico di cui l'Istituto è investito.

Possono essere attivati sistemi di videosorveglianza solo in quanto strumentali alle finalità di cui all'art. 3 o quando il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione

dei dati personali;

- **principio di necessità:** I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»). Prima di installare un sistema di videosorveglianza, il titolare del trattamento deve valutare criticamente se questa misura sia in primo luogo idonea a raggiungere l'obiettivo desiderato e, in secondo luogo, adeguata e necessaria per i suoi scopi. Si deve optare per misure di videosorveglianza unicamente se la finalità del trattamento non può ragionevolmente essere raggiunta con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato.
 - **principio di proporzionalità:** le caratteristiche dei sistemi (in particolare la dislocazione delle videocamere e le modalità di ripresa) sono definite in modo da comportare un trattamento dei soli dati pertinenti e non eccedenti rispetto alle finalità perseguite («**minimizzazione dei dati**»).
 - **principio di limitazione della conservazione:** Le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite. Il titolare ha individuato in 72 ore il periodo di tempo di conservazione ordinario delle registrazioni.
 - **principio di integrità e riservatezza:** le immagini e videoregistrazioni devono essere trattate in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
4. Laddove, per la natura dei dati trattati, per le modalità di trattamento o per gli effetti che il trattamento può determinare, emergano rischi specifici per i diritti e le libertà fondamentali degli interessati, il Titolare è tenuto ad effettuare una valutazione di impatto sulla protezione dei dati ex art. 35 del GDPR. A tal fine si consulta con il DPO e, a seconda degli esiti, prima di procedere al trattamento consulta l'autorità Garante, secondo quanto previsto all'art. 36 del GDPR.

Articolo 3 - Finalità e base giuridica

1. Il trattamento di dati personali attraverso sistemi di videosorveglianza da parte di INDIRE avviene esclusivamente nell'ambito dello svolgimento delle funzioni istituzionali e per il perseguimento di un legittimo interesse del Titolare. L'installazione di sistemi di rilevazione delle immagini da parte dell'Istituto risponde alle seguenti finalità, nel rispetto del principio di determinatezza:

- a) Tutela dei beni ed il patrimonio dell'Istituto;
- b) Prevenzione di eventuali condotte illecite e reati (furti, danneggiamenti, atti di vandalismo);
- c) Garanzia di una maggiore sicurezza al personale e ai visitatori che a vario titolo accedono agli uffici INDIRE.

Si provvede alla raccolta di dati strettamente necessari per il raggiungimento delle finalità sopra elencate, rilevando e/o registrando le sole immagini indispensabili e limitando l'angolo visuale delle riprese. L'attività di videosorveglianza e di registrazione delle immagini rilevate non è utilizzata per fini diversi da quelli esplicitati, salvo collaborazione richiesta dalle forze dell'ordine anche in base a normative o regolamenti cui sono soggette le Pubbliche Amministrazioni.

- 2. La videosorveglianza è lecita se è necessaria per conseguire la finalità di un legittimo interesse perseguito da INDIRE, a meno che su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (articolo 6, paragrafo 1, lettera f)). I legittimi interessi perseguiti da un titolare del trattamento possono avere natura giuridica, economica o immateriale. Tuttavia, il titolare del trattamento dovrebbe considerare che se l'interessato si oppone alla sorveglianza a norma dell'articolo 21, si può procedere alla videosorveglianza di tale interessato soltanto se il legittimo interesse in questione ha natura cogente e prevale sugli interessi, i diritti e le libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

In presenza di una situazione di reale rischio, la tutela della proprietà da furti o atti vandalici può costituire un legittimo interesse con riguardo alla videosorveglianza.

Articolo 4 - Personale autorizzato al trattamento

- 1. Il Titolare del trattamento di dati personali effettuato mediante i sistemi di videosorveglianza installati presso l'Istituto è INDIRE stesso, nella persona del Presidente *pro tempore*.

L'Istituto si è dotato di un proprio organigramma privacy pubblicato sul sito web istituzionale che prevede, *inter alia*, le figure del c.d. "**soggetto designato**" o "**referente privacy**", tutte le persone fisiche che operano in posizione di vertice nell'organizzazione dell'ente (addetti alla direzione di un ufficio, un reparto, un'area aziendale) e alle quali il titolare del trattamento abbia delegato specifici compiti in relazione alle operazioni di trattamento di dati personali) ed i c.d. "**soggetti autorizzati**", coloro che sono collocati al livello base dell'organigramma aziendale e

che materialmente eseguono attività di trattamento sotto l'autorità diretta del titolare o del responsabile.

Il Titolare designa, con atto scritto , **uno o più Referenti privacy per l'impianto di videosorveglianza situato presso le sedi di Firenze e di Napoli (Allegato A)**, impartisce direttive in ordine al trattamento dei dati e vigila sull'osservanza delle norme di legge, del Regolamento e delle direttive da parte del Referente privacy designato e degli autorizzati al trattamento.

Il Titolare cura i rapporti con il Garante per il tramite del proprio DPO, provvedendo in particolare a richiedere la consultazione preliminare in ordine alla legittimità del trattamento, ove ne sussistano i presupposti ai sensi dell'art. 35 GDPR.

2. Il Referente Privacy designato per la videosorveglianza effettua il trattamento attenendosi alle istruzioni impartite per iscritto dal Titolare.

In particolare, il Referente Privacy designato all'impianto di videosorveglianza:

- Supervisiona e controlla le persone fisiche autorizzate ad utilizzare gli impianti, ad accedere ai locali dove si trovano le postazioni di controllo, a visionare le immagini e ad effettuare eventuali ulteriori operazioni. Tali persone devono essere autorizzate al trattamento mediante atto sottoscritto dal Titolare contenente istruzioni per il trattamento in relazione alle sedi di Firenze e di Napoli (**Allegato B**);
- vigila sull'osservanza da parte degli Autorizzati delle norme di legge, di regolamento e delle direttive impartite;
- osserva ed assicura l'osservanza della normativa vigente in materia di videosorveglianza ed in particolare delle norme di legge, delle disposizioni del Garante, del presente Regolamento e delle direttive impartite dal Titolare;
- vigila sulla conservazione delle immagini e sulla loro cancellazione nei termini previsti dal presente Regolamento;
- riesamina in differita le immagini in caso di effettiva e comprovata necessità, per il conseguimento delle finalità indicate all'art. 3 del presente Regolamento; nel caso di riesame di immagini relative all'area CED che riprendano anche il personale tecnico eventualmente ivi presente, ne dà informazione alle OO.SS. e alle RSU, al fine di avere la presenza di un rappresentante delle OO.SS. al riesame;
- vigila sulla manutenzione ordinaria e straordinaria dei sistemi da parte degli Autorizzati o, ove necessario, di personale esterno, garantendo l'osservanza della normativa vigente e del presente Regolamento da parte di chi entri in contatto con

i dati registrati;

- provvede a far sì che venga installata la segnaletica di avvertimento in modalità chiaramente visibile da chiunque acceda negli spazi videosorvegliati, collocandola prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente in prossimità della stessa. In relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli segnaletici;
 - Gestisce e sovrintende il procedimento di accesso alle immagini da parte dei soggetti interessati, in collaborazione con il DPO dell'Istituto;
3. I soggetti autorizzati ad utilizzare gli impianti e a visionare le registrazioni svolgono le operazioni materiali di trattamento attenendosi alle istruzioni impartite dal Titolare che provvede ad aggiornarle in caso di modifiche organizzative, tecniche e normative.

Articolo 5 – Modalità di trattamento delle immagini

1. Le caratteristiche tecniche degli impianti di videosorveglianza sono descritte in appositi documenti, assieme all'ubicazione delle telecamere, alle modalità di rilevazione, accesso e conservazione delle registrazioni (**Allegato C e Allegato C1 per l'impianto di via Lombroso, Firenze – Allegato D e Allegato D1 per l'impianto di Via Buonarroti, Firenze – Allegato E e Allegato E1 per l'impianto di Napoli in via Melisurgo**). I documenti sono conservati a cura del Referente privacy designato alla videosorveglianza che provvede al loro aggiornamento. Per esigenze particolari, il Referente Privacy designato può proporre al Titolare, sentito il Responsabile della protezione dati, disposizioni in deroga rispetto a quelle descritte nel presente documento. In ragione di sopraggiunte novità tecnologiche e/o esigenze rispondenti alle finalità di cui al precedente art. 3), o per proposte approvate di cui al precedente capoverso, il Titolare del trattamento dei dati provvederà a modificare o integrare i documenti nel rispetto di quanto previsto dal presente Regolamento, previa eventuale informazione alle OO.SS., alle RSU e agli organi competenti.
2. Le videocamere installate consentono unicamente riprese video; non effettuano riprese audiofoniche.

Impianto di Via Lombroso

Le telecamere di sicurezza, come meglio precisato negli Allegati C e C1, sono installate esternamente, con funzione *night & day*, e sono disposte sul perimetro della sede di Firenze al piano terra (3 lato via Lombroso e 3 Lato via Cisalpino) ed 1 telecamera è posta sulla scalinata esterna che conduce al piano superiore dove si accede all'Agenzia Nazionale Erasmus+.

Vi sono inoltre un paio di telecamere installate all'interno della sala CED della sede di Firenze di Via Lombroso per controllo accessi e controllo da remoto degli stati delle macchine installate. In caso di riesame delle immagini riferite a tale locale valgono le disposizioni di cui all'art. 4 del presente Regolamento.

Impianto di Via Buonarroti

Le 3 telecamere di sicurezza sono installate esternamente al complesso, con funzione *night & day*, sono disposte sul perimetro della sede, (una disposta al lato giardino Comunale "Chelazzi" in Via Dell' Agnolo, 53, una nel lato giardino Comunale Piazza dei Ciompi e una disposta sul portone principale d'ingresso della sede Via Buonarroti, 10) tutte sono orientate sulle uscite di emergenza e sull'ingresso principale.

Impianto di via Melisurgo

La telecamera installata all'interno della sede INDIRE ed Erasmus+ di Via Melisurgo 4, Napoli, riprende esclusivamente l'ingresso dell'ufficio e il quadro rack della rete dati e la centrale antincendio.

3. Non devono essere installate apparecchiature specificamente preordinate al controllo a distanza dell'attività del personale INDIRE e di tutti coloro che accedono a vario titolo all'interno dei locali dell'Istituto, non devono essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza, il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa o dell'attività diversa espletata.

4. I trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti dall'art. 32 del GDPR, nel Provvedimento generale e nelle Linee Guida EDPB, secondo i principi richiamati all'art. 2 del presente Regolamento.

L'accesso alla sala tecnica ove sono situate le apparecchiature di registrazione e le

postazioni di controllo è consentito esclusivamente, in via ordinaria, al Titolare, al/i Referente Privacy designato/i e al personale a ciò autorizzato mediante incarico nonché al personale di pubblica sicurezza o di polizia giudiziaria. Il personale adibito al servizio di pulizia può accedervi per il tempo strettamente necessario all'espletamento delle proprie mansioni e con la preclusione alla visione delle immagini. L'accesso di soggetti diversi da quelli indicati può avvenire solo in via eccezionale, per comprovata necessità in relazione alle finalità indicate nell'art. 3 e previa autorizzazione del Titolare o del Referente Privacy designato.

Articolo 6 - Conservazione

1. Le immagini dell'impianto di Via Lombroso sono conservate in una *control room* ad accesso protetto ubicata presso la sede di INDIRE sita in Via Lombroso (Firenze) per un periodo di tempo pari a 72 ore, fatte salve esigenze di ulteriore conservazione in caso di eventuali richieste da parte delle autorità giudiziarie o delle FF.OO. L'archiviazione delle immagini è protetta da password.
2. Le immagini dell'impianto di Via Buonarroti sono conservate in un DVR posto all'interno della *control room* ad accesso protetto (chiusa a chiave con serratura elettronica con apertura automatica attraverso un badge in possesso di personale autorizzato e istruito) ubicata al terzo piano all'interno della sala CED presso la sede di INDIRE sita in Via Buonarroti, per un periodo di tempo pari a 72 ore, fatte salve esigenze di ulteriore conservazione in caso di eventuali richieste da parte delle autorità giudiziarie o delle FF.OO. L'archiviazione delle immagini è protetta da password.

Per i periodi di chiusura programmata delle sedi INDIRE, nonché nelle ipotesi di rischio concreto, la conservazione per un tempo superiore alle 72 ore dalla registrazione può avvenire argomentando in maniera motivata la legittimità dello scopo del trattamento e la necessità della conservazione per un tempo maggiore

3. Le immagini della sede di via Melisurgo non vengono registrate nè conservate. E' abilitata soltanto la ripresa live, negli orari di chiusura dell'ufficio. La telecamera infatti entra in funzione esclusivamente all'attivazione dell'impianto di allarme antintrusione. La visione delle immagini è prevista solo in modalità LIVE, accessibili da apposita app, mediante inserimento di una password.

Art. 7 - Misure di sicurezza

I dati raccolti mediante i sistemi di videosorveglianza sono protetti, ai sensi dell'art. 32 del GDPR con idonee e preventive misure di sicurezza, al fine di ridurre al minimo i rischi di distruzione, perdita anche accidentale, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini e alla loro conservazione entro i tempi individuati. In particolare, sono adottate le seguenti misure tecniche e organizzative:

- 1) il Referente Privacy designato e gli Autorizzati, nell'ambito dei compiti attribuiti a ciascuno, utilizzano credenziali di autenticazione strettamente personali che permettono di effettuare unicamente le operazioni di propria competenza;
- 2) la possibilità, per i soggetti abilitati, di visionare le immagini in tempo differito, è limitata ai casi di effettiva e documentata necessità, per il conseguimento delle finalità indicate all'art. 3 del presente Regolamento;
- 3) i sistemi di videosorveglianza delle sedi di Firenze sono configurati in modo tale da consentire la cancellazione automatica delle immagini registrate dal supporto, allo scadere del termine di conservazione stabilito ai sensi dell'art. 6 del presente Regolamento, anche mediante sovra-registrazione e con modalità tali da rendere inutilizzabili i dati cancellati, così come descritte nel documento di cui al precedente art. 5 comma 1;
- 4) I dispositivi di registrazione previsti per gli impianti delle sedi di Firenze si trovano in locali ad accesso protetto e l'archiviazione delle immagini è protetta da password.
- 5) nel caso di interventi derivanti da esigenze di manutenzione, i soggetti preposti potranno accedere alle immagini solo se ciò è indispensabile al fine di effettuare eventuali verifiche tecniche, ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini e per il solo tempo necessario all'intervento di manutenzione;
- 6) deve essere consentito al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa.
- 7) Misure che garantiscono il controllo degli accessi e la sicurezza del sistema di videosorveglianza e dei dati.

Art. 8 - Comunicazione delle immagini/videoregistrazioni

1. La comunicazione ad altri soggetti pubblici dei dati personali acquisiti mediante i sistemi di videosorveglianza è ammessa solo se prevista da norma di legge o di regolamento, come meglio disciplinato dall'art. 2ter del Codice Privacy.
2. La comunicazione di videoregistrazioni alle autorità di contrasto è un processo indipendente, per il quale INDIRE deve individuare una separata giustificazione. Secondo l'articolo 6, paragrafo 1, lettera c) del GDPR, il trattamento è lecito se è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento. IL D.P.R. 15 gennaio 2018, n. 15 ha emanato il *"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"*.
3. Per finalità di polizia si intendono *"i trattamenti correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati"*
4. In caso di richiesta di accesso alle immagini/videoregistrazioni effettuata dalle FF.OO per finalità di polizia INDIRE è tenuta a comunicare tali informazioni.
5. In caso di cooperazione con le autorità di contrasto (per esempio nelle indagini), la base giuridica per la trasmissione dei dati consiste in un obbligo legale di cui all'articolo 6, paragrafo 1, lettera c).
6. Non è consentita la diffusione delle registrazioni acquisite mediante i sistemi di videosorveglianza.

Articolo 9 - Nuove attivazioni o revisioni dei sistemi di videosorveglianza

In caso di subentrante esigenze per le quali si rendesse necessaria la realizzazione di nuovi sistemi di videosorveglianza, o la sostituzione di quelli esistenti con impianti di tecnologia avente caratteristiche diverse dalla preesistente, il Referente Privacy designato alla videosorveglianza è obbligato a darne preventiva comunicazione al Titolare e al Responsabile della protezione dati di INDIRE.

Tale comunicazione si rende necessaria per consentire al Titolare il rispetto degli obblighi previsti all'art. 25 GDPR inerenti la protezione dei dati fin dalla progettazione e

l'attivazione delle verifiche di cui all'art. 2 punto 4 del presente regolamento.

In tal caso, previa eventuale intesa con le OO.SS, si provvederà ad un aggiornamento del presente regolamento.

Art. 10 - Obblighi di trasparenza e informazione

Gli interessati devono essere preventivamente informati che stanno per accedere ad una zona sottoposta a videosorveglianza. Le informazioni più importanti devono essere indicate sul segnale/cartello di avvertimento stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello). A tale scopo INDIRE:

1. Informa gli interessati in ordine alla presenza in alcune aree di sistemi di videosorveglianza mediante l'affissione, in prossimità delle videocamere e degli accessi alle aree videosorvegliate, del modello di informativa (**Allegato F, Allegato F1, Allegato F2**) indicante, *inter alia*, ai sensi dell'art.13 del GDPR:
 - a. il Titolare del trattamento;
 - b. il Responsabile della protezione dati;
 - c. le finalità perseguite;
 - d. le basi giuridiche del trattamento;
 - e. il rinvio all'informativa estesa.
2. Colloca l'informativa prima del raggio di ciascuna videocamera, eventualmente con più cartelli, in posizione che ne garantisca la visibilità in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza è attivo in orario notturno. Le informazioni devono essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi). Non è necessario rivelare l'ubicazione della telecamera, purché non vi siano dubbi su quali zone sono soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza. L'interessato deve poter stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.
3. Mette a disposizione degli interessati sul proprio sito internet istituzionale, mediante affissione in bacheca e presso la portineria/guardiania delle sedi dove

è presente un impianto di videosorveglianza, il testo completo dell'informativa integrale (di secondo livello), contenente tutti gli elementi previsti all'art. 13 GDPR (**Allegato G, Allegato G1, Allegato G2**) e meglio chiariti nelle Linee Guida EDPB

Articolo 11 – Diritti degli interessati

1. Ai soggetti interessati, così come definiti all'art. 1, è assicurato l'esercizio dei diritti in conformità agli artt. 15 (diritto di accesso), 17 (diritto alla cancellazione), 18 (diritto di limitazione di trattamento), e 21 (diritto di opposizione) del GDPR fermo restando che, in taluni casi potrebbero risultare non consentite azioni di cancellazione né l'opposizione al trattamento, come previsto al paragrafo 1 art. 21 GDPR.
2. La risposta ad una richiesta di accesso ai dati da parte dell'interessato può comprendere eventuali dati riferiti a terzi nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato, purché non risulti lesivo dei diritti e delle libertà altrui.
3. Le informazioni complete per l'esercizio dei diritti sono riportate nell'informativa.

Articolo 12 – Diritto di accesso

1. Un interessato ha diritto di ottenere dal titolare del trattamento la conferma o meno del fatto che i propri dati personali siano oggetto di trattamento. Per quanto riguarda la videosorveglianza, ciò significa che se nessun dato è conservato o trasferito, una volta trascorso il momento del monitoraggio in tempo reale, il Titolare potrebbe soltanto comunicare che nessun dato personale è più oggetto di trattamento. Se tuttavia i dati sono ancora in corso di trattamento al momento della richiesta (vale a dire se i dati sono conservati o trattati ininterrottamente in qualsiasi altro modo), l'interessato dovrebbe ricevere accesso e informazioni conformemente alle disposizioni dell'articolo 15 del GDPR.
2. Esistono, tuttavia, alcune limitazioni che in determinati casi possono trovare applicazione rispetto al diritto di accesso.

▪ Articolo 15, paragrafo 4, del GDPR – Ledere i diritti altrui

Poiché nella stessa sequenza di videosorveglianza può essere registrato un numero qualsiasi di interessati, uno screening comporterebbe un ulteriore trattamento dei dati personali di altri interessati. Se l'interessato desidera ricevere una copia del materiale

(articolo 15, paragrafo 3), ciò potrebbe ledere i diritti e le libertà di altri soggetti che compaiono nella registrazione. Per evitare tale rischio, il titolare del trattamento dovrebbe quindi tenere conto del fatto che, a causa della natura intrusiva delle riprese video, in alcuni casi non dovrebbe fornire riprese video in cui siano identificabili altri interessati. Tuttavia, la protezione dei diritti di terzi non dovrebbe essere utilizzata come pretesto per impedire legittime richieste di accesso; in questi casi, il titolare del trattamento dovrebbe porre in atto misure tecniche per soddisfare la richiesta di accesso (ad esempio, modifica delle immagini tramite mascheramento o crittografia). Tuttavia, i titolari del trattamento non sono obbligati ad attuare tali misure tecniche se possono garantire in altro modo di rispondere a una richiesta ai sensi dell'articolo 15 entro il termine stabilito dall'articolo 12, paragrafo 3.

- Articolo 11, paragrafo 2, del GDPR – Il titolare del trattamento non è in grado di identificare l'interessato

Se nel filmato non è possibile effettuare una ricerca di dati personali (vale a dire che il titolare del trattamento probabilmente dovrebbe analizzare una grande quantità di materiale conservato per trovare l'interessato in questione), il titolare del trattamento potrebbe non essere in grado di identificare l'interessato.

Per questi motivi, nella sua richiesta al titolare del trattamento l'interessato dovrebbe (oltre a identificarsi anche con un documento d'identità o di persona) specificare quando – entro un lasso di tempo ragionevole in proporzione alla quantità di interessati registrati – è entrato nella zona sorvegliata. Il titolare del trattamento dovrebbe notificare preventivamente all'interessato di quali informazioni ha bisogno per poter soddisfare la richiesta. Se il titolare del trattamento può dimostrare di non essere in grado di identificare l'interessato, ne informa quest'ultimo, ove possibile. In un caso del genere, il titolare del trattamento dovrebbe informare l'interessato nella risposta circa la zona specificamente soggetta a sorveglianza, la verifica delle telecamere in uso, ecc., in modo che l'interessato comprenda esattamente quali dei suoi dati personali possano essere stati trattati.

3. Il diritto di accesso alle immagini acquisite mediante i sistemi di videosorveglianza e conservate presso l'Istituto, da parte dell'interessato o per la tutela di situazioni giuridicamente rilevanti, si esercita con istanza scritta (**Allegato H e Allegato H1**) e motivata presentata al Titolare o al Referente Privacy designato alla videosorveglianza e al Responsabile della protezione dati; è disciplinato rispettivamente dal GDPR e dal Codice Privacy

Articolo 13 – Entrata in vigore

1. Il presente Regolamento è approvato con delibera del CDA ed entra in vigore il giorno successivo alla sua pubblicazione. Il presente regolamento è soggetto ad aggiornamenti periodici.

Articolo 14 – Allegati

Gli allegati costituiscono parte integrante e sostanziale del presente regolamento sulla videosorveglianza.

- A. Modello Atto di designazione referente privacy videosorveglianza da personalizzare per sede
- B. Modello Atto di designazione persona autorizzata al trattamento (soggetto autorizzato alla visione immagini in tempo reale; soggetto autorizzato alla visione immagini registrate e accesso control room; soggetto autorizzato alla custodia delle credenziali di autenticazione per accedere al DVR) da personalizzare per sede
- C. Relazione tecnica funzionamento impianto di videosorveglianza con ubicazione telecamere sede di Firenze, Via Lombroso;
 - C1. Planimetria impianto di videosorveglianza sede di Firenze, Via Lombroso;
- D. Relazione tecnica funzionamento impianto di videosorveglianza con ubicazione telecamere sede di Firenze, Via Buonarroti;
 - D1. Planimetria impianto di videosorveglianza sede di Firenze, Via Buonarroti;
- E. Relazione tecnica funzionamento impianto di videosorveglianza con ubicazione telecamere sede di Napoli, Via Melisurgo;
 - E1. Planimetria impianto di videosorveglianza sede di Napoli, Via Melisurgo;
- F. Informativa semplificata (segnale di avvertimento di primo livello) presso sede Via Lombroso;
 - F1. Informativa semplificata (segnale di avvertimento di primo livello) presso sede Via Buonarroti;
 - F2. Informativa semplificata (segnale di avvertimento di primo livello) presso sede via Melisurgo;

G. Informativa integrale presso sede via Lombroso;

G1. Informativa integrale presso sede via Buonarroti;

G2. Informativa integrale presso sede Via Melisurgo;

H. Modello istanza di accesso alle immagini via Lombroso;

H1. Modello istanza di accesso alle immagini via Buonarroti;