Regolamento Videosorveglianza

(approvato con deliberazione del C.d.A. n. 14 del 21.03.2023)

INDICE

1 - PREMESSE

Il presente regolamento disciplina l'esercizio degli impianti di videosorveglianza installati presso l'I.P.A.B. in conformità a quanto stabilito dalla normativa in materia di trattamento dei dati personali, dando attuazione ai principi di liceità, necessità, proporzionalità e finalità previsti dalla normativa in materia di protezione dei dati personali.

L'attività di videosorveglianza viene svolta con la finalità per garantire la sicurezza degli utenti, del personale e dei visitatori e la tutela del patrimonio dell'Ente ed evitare il furto di farmaci, apparecchiature mediche/sanitarie o altri beni strumentali dell'Ente.

L'Ente intende eseguire i trattamenti in materia di videosorveglianza nel rispetto del Provvedimento generale sulla videosorveglianza emanato l'8 aprile 2010, del Codice in materia di protezione dei dati personali (D.Lgs.196/2003, modificato col D.Lgs 101/2018 del Regolamento Europeo in materia di protezione dei dati personali 2016/679.

Con il presente atto l'Ente intende fornire un'adeguata documentazione delle ragioni delle scelte riguardo i trattamenti di videosorveglianza e le misure adottate, anche ai fini dell'eventuale utilizzazione ed esibizione di tale documentazione in occasione di visite ispettive, oppure dell'esercizio dei diritti degli interessati o di legittimo interesse del Titolare del trattamento.

Il presente documento verrà tempo per tempo aggiornato in ragione delle eventuali, ulteriori modificazioni che interverranno riguardo alle attività e sistemi di videosorveglianza.

L'Ente tratterà i dati personali nell'ambito delle finalità previste con rispetto dei diritti e delle libertà fondamentali dei cittadini, della dignità delle persone con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati stessi.

Il trattamento delle immagini da parte dell'Ente avverrà nel rispetto dalle disposizioni di Legge relativamente all'installazione di apparecchi audiovisivi (norme civili e penali in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela e dallo Statuto dei lavoratori, legge 300/1970.

Il trattamento dei dati effettuato tramite impianto di videosorveglianza utilizzato dall'I.P.A.B. è stato sottoposto a Valutazione d'Impatto sulla protezione dei dati e non sono stati rilevati rischi importanti per i diritti e libertà degli interessati.

2 – NORMATIVE DI RIFERIMENTO

Il presente Regolamento è stato redatto in conformità alle seguenti disposizioni:

- Provvedimento generale in materia di Videosorveglianza dell'8/4/2010;
- Statuto dei lavoratori, Legge 300/70.
- Codice in materia di protezione dei dati personali, D.Lgs.196/2003 modificato con il D.Lgs.101/2018;
- Regolamento Europeo in materia di protezione dei dati personali 2016/679, di seguito GDPR;

3 - DEFINIZIONI

Di seguito si riportano le definizioni dei termini impiegati conformi a quanto specificato nel GDPR:

Interessato: la persona fisica, cui si riferiscono i dati personali.

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;

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato.

Categorie particolari di dati: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dati giudiziari: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

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;

Titolare del trattamento (anche "Titolare"): 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;

quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Responsabile del trattamento (anche "Responsabile"): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Autorizzato o Incaricato: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

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 dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

4 – IDENTIFICAZIONE DEI RUOLI PREVISTI DAL REGOLAMENTO EUROPEO 2016/679

Titolare del trattamento: I.P.A.B. di Vicenza è Titolare del trattamento, nella persona del Presidente, Legale Rappresentante, ivi elettivamente domiciliato.

Responsabile del trattamento: Il Titolare individua nella persona del Direttore Generale dell'Ente il Responsabile del trattamento, delegandolo allo svolgimento di tutti gli adempimenti previsti dalla normativa.

Incaricati: il Titolare o su sua delega il Responsabile identifica e nomina gli incaricati del trattamento definendo in maniera puntuale ruoli. Si definiranno idonee regole di accesso ai dati trattati per consentire agli incaricati di conseguire i risultati previsti dai ruoli identificati.

Riferimenti del Responsabile della protezione dei dati: l'indirizzo di posta elettronica allo scopo creata relativa al responsabile della protezione dei dati, nominato dal Titolare in conformità del GDPR sarà riportato sulle informative predisposte.

5 – PRINCIPI GENERALI

Il Titolare ha deciso di conformare la configurazione del sistema di videosorveglianza adottato ai principi definiti dal GDPR e fatti propri dalla Autorità garante.

Si definiscono:

- Finalità del trattamento.
- Principio di liceità;
- Principio di necessità;
- Principio di proporzionalità;
- Necessità di informativa e consenso degli interessati.

Finalità del trattamento

I trattamenti oggetto del presente Regolamento saranno svolti al fine di tutelare la sicurezza ed i beni dei lavoratori, degli ospiti e dei visitatori dei locali dell'Ente, prevenire atti vandalici e tutelare il patrimonio dell'Ente.

Principio di Liceità

I dati saranno trattati in maniera lecita nel rispetto delle prescrizioni normative da incaricati allo scopo identificati e nominati dall'Ente in qualità di Titolare del trattamento.

Il Titolare adotterà disposizioni tecniche ed organizzative idonee a garantire la protezione dei dati trattati.

Principio di Necessità

I dati saranno trattati esclusivamente per conseguire le finalità indicate nel rispetto delle motivazioni indicate.

Principio di Proporzionalità

Gli strumenti adottati e le procedure implementate garantiscono il rispetto del principio di proporzionalità al fine di impedire trattamenti eccedenti rispetto alle finalità indicate.

Necessità di informativa e consenso degli interessati

Il Titolare disporrà, nel rispetto della normativa vigente, idonei cartelli informativi della presenza dei sistemi di videosorveglianza.

Il Titolare rende disponibile presso i servizi di portineria e la segreteria l'informativa completa sui trattamenti svolti.

6 – SPECIFICHE TECNICHE GENERALI

In conformità a quanto previsto dalla normativa il Titolare predisporrà la documentazione di progetto così composta:

Identificazione delle aree interessate alle riprese

Su predisporranno piantine delle aree interessate alle riprese riportanti la posizione, l'orientamento e l'angolo di ripresa di ogni telecamera.

Ad ogni telecamera sarà assegnato un codice identificativo univoco.

Definizione delle caratteristiche delle telecamere

Per ogni telecamera identificata al punto precedente si predisporrà una scheda riportante i dati identificativi, le caratteristiche tecniche e le principali funzioni quali, ad esempio, la possibilità di riprese notturne, capacità di lettura di scritte, capacità di riconoscimento del movimento, risoluzione, ripresa a colori o in bianco e nero, funzioni di zoom automatico o possibilità di controllo a distanza.

Strumenti di registrazione delle riprese

Gli strumenti di conservazione delle riprese dovranno essere realizzati nel rispetto dei principi di affidabilità e aderenza ai principi del GDPR.

Luogo di installazione e conservazione degli apparati di registrazione: gli apparati dovranno essere posti in aree ad accesso controllato e si dovrà garantire la protezione di accesso ai dati mediante credenziali personali con password con scadenza e complessità conformi alle definizioni di sicurezza adottate dal Titolare.

Alle credenziali dovranno essere associati diritti di accesso ai dati conformi alle finalità identificate per ogni incaricato.

Tempo di conservazione delle registrazioni

Le registrazioni saranno conservate per un tempo di 7 giorni.

Modalità di cancellazione

Le registrazioni saranno cancellate dai sistemi di registrazione allo scadere del tempo di conservazione previsto.

Protezione dei dati

Il Responsabile del trattamento in coordinamento col responsabile della gestione dei sistemi informatici provvederà ad implementare le misure tecniche ed organizzative idonee a garantire la protezione da accessi fraudolenti dei dati trattati, dalla loro perdita o manomissione da parte di terzi.

Posizionamento dei monitor

I monitor per la visione in tempo reale delle immagini dovranno essere collocati in modo tale da non permettere la visione a persone non autorizzate.

7 – PROCEDURE E NORME DI COMPORTAMENTO

Assegnazione delle credenziali di accesso

Le credenziali di accesso ai sistemi saranno rilasciate dal responsabile della gestione dei sistemi informatici su indicazione del Responsabile del trattamento.

La richiesta di assegnazione dovrà specificare il nominativo dell'incaricato e le autorizzazioni che dovranno essere assegnate.

Conservazione ed utilizzo delle credenziali

Le credenziali sono personali e dovranno essere conservate con la massima cura da parte degli incaricati.

In nessun caso e per nessuna motivazione le credenziali potranno essere comunicate a terzi.

In caso di necessità l'accesso da parte di terzi non potrà avvenire con credenziali già assegnate.

Il Titolare potrà creare una credenziale di accesso con privilegi amministrativi che sarà conservata in busta sigillata e luogo sicuro a cura del Titolare al fine di garantire l'accesso ai sistemi in caso di necessità. Una volta utilizzate tali credenziali dovranno essere annullate e sostituite con nuove credenziali.

Revoca delle credenziali

Il Responsabile del trattamento indicherà al responsabile della gestione dei sistemi informatici la necessità di procedere alla revoca delle credenziali.

Accesso alla registrazione delle immagini

L'accesso alle registrazioni potrà avvenire esclusivamente su richiesta della Autorità giudiziaria.

In caso di richiesta di conservazione delle immagini da parte delle autorità inquirenti il responsabile della gestione dei sistemi informatici provvederà a realizzare una copia delle immagini che sarà firmato in modo digitale al fine di garantire la data ed ora della esecuzione della copia e garantendone l'immodificabilità del contenuto.

Il file dovrà essere conservato con modalità tali da garantirne l'impossibilità ad accedere se non in presenza della Autorità giudiziaria.

Nel caso si rendesse necessaria la sostituzione del supporto di conservazione delle registrazioni si dovrà procedere alla distruzione fisica del supporto sostituito.

Accesso mediante dispositivi mobili o remoti

L'accesso ai dati ed ai sistemi di registrazione mediante dispositivi mobili o remoti potrà avvenire esclusivamente mediante protocolli e sistemi di protezione della connessione che garantiscano la sicurezza del traffico impedendo la violazione della sicurezza dei dati. Le credenziali di accesso dall'esterno dovranno essere differenti da quelle assegnate per l'accesso ai sistemi di videoregistrazione ed univoche.

Log dell'accesso ai sistemi

In conformità da quanto previsto dalle disposizioni della Autorità garante l'accesso ai sistemi dovrà essere conservato mediante file di log immodificabili e conservati per un periodo minimo di sei mesi.

8 – DEFINIZIONE DEI RUOLI

Si identificano i seguenti ruoli che saranno assegnati agli incaricati a cura del Responsabile del trattamento.

In funzione dei ruoli identificati saranno assegnate i relativi privilegio di accesso al sistema.

Addetti alla gestione dei sistemi e Amministratori di sistema: a tale ruolo appartengono gli incaricati della installazione, configurazione e manutenzione dei sistemi di ripresa, degli impianti di connessione, dei sistemi di registrazione e protezione.

Ogni incaricato per la parte di competenza dovrà essere nominato o come incaricato o come Responsabile esterno ai sensi dell'articolo 28 del GDPR.

In caso di necessità potrà essere nominato amministratore di sistema.

Autorizzati all'accesso alle registrazioni: a tale ruolo appartengono gli incaricati con credenziali idonee ad accedere alle registrazioni ed eventualmente a predisporre le copie richieste dalla Autorità giudiziaria. L'accesso alle registrazioni avverrà esclusivamente nel rispetto delle normative esistenti e sotto la supervisione del Responsabile del trattamento.

Incaricati alla visualizzazione delle immagini: Il personale che potrà avere accesso alle riprese in tempo reale delle immagini saranno identificati a cura del Responsabile del trattamento ed allo scopo formati al fine di garantire un uso degli strumenti conformi ai principi del GDPR.

9 – ADEMPIMENTI AI SENSI DEL REGOLAMENTO EUROPEO 2016/679

Predisposizione e mantenimento della documentazione prevista

Il Responsabile del trattamento provvederà alla predisposizione del Registro dei trattamenti ed alla valutazione dei rischi relativi ai trattamenti svolti.

I documenti saranno sottoposti a revisione periodica secondo le modalità definite dal Responsabile del trattamento.

Formazione degli incaricati: Il Titolare del trattamento valuterà i fabbisogni formativi degli incaricati in funzione dei ruoli e delle finalità assegnate.

10 – AUTORIZZAZIONE ALLA INSTALLAZIONE DEI SISTEMI DI VIDEOSORVEGLIANZA

L'installazione dei sistemi di videosorveglianza avverrà nel rispetto del conseguimento delle approvazioni previste da parte delle Rappresentanze sindacali dell'Ente e dell'Ispettorato del Lavoro.

Tali approvazioni dovranno essere conseguite preventivamente alla installazione ed attivazione dei sistemi.

11 – ACCESSO ALLE REGISTRAZIONI DA PARTE DI TERZI

L'accesso alle registrazioni delle immagini è possibile esclusivamente da parte della Autorità giudiziaria.

Pertanto, non è consentito l'accesso alle registrazioni da parte di terzi o di incaricati se non a seguito della presentazione di denuncia alle autorità competenti.

12 – ESCLUSIONI

Si esclude l'utilizzo delle immagini trattate per finalità differenti da quelle specificate nel presente Regolamento, fatte salve differenti indicazioni da parte della Autorità giudiziaria.

In nessun caso, le immagini saranno impiegate per finalità di controllo del personale o di tutti coloro che collaborano con l'Ente.