UNIVERSITÀ DI PAVIA

Servizio Legale
UOC Privacy, anticorruzione e trasparenza

Pavia, [1]

Protocollo n.: [1]
Titolo I - Classe 6
Fascicolo 2021

Ai Responsabili interni del trattamento

LORO SEDI

Oggetto: Disciplinare sull'impiego di sistemi di videosorveglianza negli ambienti dell'Università degli Studi di Pavia.

Gentilissimi,

in attuazione del Regolamento (UE) 2016/679 (RGPD) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e del D. Lgs. n. 196/2003, come novellato dal D. Lgs. n. 101/2018, l'Università degli Studi di Pavia, in qualità di Titolare del Trattamento, ha adottato, con la Determinazione Dirigenziale rep. 1117/2021 Prot. n.64116 del 10/05/2021, il *"Disciplinare sull'impiego di sistemi di videosorveglianza negli ambienti dell'Università degli Studi di Pavia"* quivi allegato, finalizzato a fornire indicazioni sull'applicazione del RGPD in relazione al trattamento di dati personali attraverso dispositivi video al fine di garantire il rispetto della normativa.
Il trattamento dei dati personali, effettuato mediante l'istallazione di sistemi di rilevazione delle immagini all'interno delle strutture universitarie, risponde a finalità determinate, esplicite e legittime quali:

- aumentare la sicurezza e incolumità del personale universitario, degli studenti e dei frequentatori a vario titolo degli spazi universitari;

- tutelare il patrimonio mobiliare e immobiliare dell'Ateneo;

- prevenire atti vandalici in assenza di altri strumenti idonei.

L'Università assicura che le immagini non siano in alcun modo impiegate come strumento di sorveglianza a distanza dei docenti, del personale tecnico – amministrativo e CEL, degli studenti e degli altri utenti dell'Ateneo (divieto prescritto dall'art 4 della Legge n. 300/1970 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento).

I Responsabili interni del trattamento, quali soggetti appositamente designati sulla scorta del dell'assetto organizzativo dell'Ateneo, sono tenuti a:

a) predisporre, aggiornare e conservare agli atti una documentazione delle scelte, in cui vengono adeguatamente spiegate le ragioni del ricorso alla videosorveglianza;

[1]data e numero di protocollo sono quelli attribuiti dalla procedura informatica all'atto della protocollazione della lettera

b) inserire e aggiornare il trattamento nel registro dei trattamenti d'Ateneo;
c) acquisire dall'installatore la dichiarazione che l'impianto è conforme alle norme previste dal RGPD, dal Codice e dalla normativa;
d) perfezionare l'accordo di designazione a responsabile esterno al trattamento del fornitore del servizio qualora ne ricorrano i presupposti;
e) individuare i soggetti autorizzati a compiere operazioni di trattamento e definire i profili di abilitazione per l'accesso alle immagini (preposti ad utilizzare gli impianti, visualizzare le immagini, ad accedere ai locali dove si trovano le postazioni di controllo e ad effettuare eventuali ulteriori operazioni) fornendo agli stessi istruzioni per il corretto trattamento dei dati, fermo restando l'accesso consentito alla polizia giudiziaria, nei casi espressamente previsti per motivi di ordine pubblico, sicurezza, tutela del patrimonio e repressione dei reati;
f) vigilare sulla conservazione delle immagini e sulla loro cancellazione nei termini previsti dal disciplinare;
g) riesaminare in differita le immagini in caso di effettiva necessità, per il conseguimento delle finalità indicate all'art. 4 del presente disciplinare;
h) vigilare sulla manutenzione ordinaria e straordinaria dei sistemi, garantendo l'osservanza della normativa vigente e del presente disciplinare da parte di chi entri in contatto con i dati registrati;
i) monitorare periodicamente gli impianti di videosorveglianza per verificare le misure per garantire la sicurezza dei dati
j) provvedere in ordine all'installazione della segnaletica in prossimità dell'impianto di videosorveglianza (cfr. all.A);
k) presidiare il monitoraggio dell'informativa semplificata tramite cartellonistica e dell'informativa per esteso (cfr. all.B);
l) garantire l'esercizio dei diritti degli interessati predisponendo ogni adempimento organizzativo necessario;
m) individuare e designare una o più persone di riferimento (*Referenti Privacy*) che avranno il compito di supporto per gli adempimenti previsti dalla normativa vigente;
n) designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
o) raccogliere ogni segnalazione di violazione di dati personali da parte di dipendenti, collaboratori e/o interessati e comunicarla tempestivamente al Responsabile della Protezione dei Dati e al Titolare secondo la procedura di segnalazione della violazione di dati personali (data breach) adottata dall'Ateneo;
p) effettuare preventiva valutazione d'impatto nei casi previsti secondo la procedura adottata dall'Ateneo e, ove i risultati della valutazione d'impatto sulla protezione dei dati indichino che il trattamento comporterebbe un rischio elevato nonostante le misure di sicurezza pianificate, informare il Titolare;
q) In caso di dismissione dell'impianto per motivi di costi, obsolescenza e sicurezza attivare tutte le procedure tecniche per la cancellazione sicura dei dati e relative copie nella disponibilità dell'ente.

Si informa che gli impianti esistenti saranno oggetto di un audit interno propedeutico alla gestione del servizio a cura del Servizio Legale, UOC Privacy, anticorruzione e trasparenza.

Si raccomanda in primo luogo di verificare la presenza dell'informativa, il periodo di cancellazione

delle immagini e limitare l'accesso agli archivi in cui sono conservate le immagini registrate ai soli soggetti autorizzati.

Nel ringraziare per la collaborazione, si porgono cordiali saluti.

Distinti saluti.

Il Responsabile del Servizio Legale
Avv. Marco Podini
(documento firmato digitalmente)

Allegati:

1. Disciplinare sull'impiego di sistemi di videosorveglianza negli ambienti dell'Università degli Studi di Pavia

A. Cartellonistica
B. Informativa estesa

MP/NP

UNIVERSITÀ DI PAVIA

Servizio Legale
UOC Privacy, anticorruzione e trasparenza

Pavia, (1) Determinazione n°, (1) Protocollo. n., (1) Titolo —– Classe — Fascicolo Allegati n.-1	OGGETTO: Disciplinare sull'impiego di sistemi di videosorveglianza negli ambienti dell'Università degli Studi di Pavia

(1) Il numero e la data di protocollo sono quelli attribuiti dalla procedura informatica all'atto della protocollazione della determina.

IL DIRETTORE GENERALE

- VISTO lo Statuto dell'Università degli Studi di Pavia ed in particolare gli articoli 17, 63 e 69;
- VISTO il Regolamento (UE) 27.04.2016, n. 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);
- VISTO il D. Lgs. 10.08.2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)";
- RICHIAMATI i provvedimenti attuativi del Regolamento (UE) 2016/676 emanati dall'Autorità Garante
per la protezione dei dati personali;
- VISTO il provvedimento del Garante Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 27 novembre 2008 (modificato in base al provvedimento del 25 giugno 2009);
-- VISTO il Provvedimento del Garante 8/4/2010;
- VISTE le Linee guida EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video versione 2.0 Adottate il 29 gennaio 2020;
- VISTO il "Modello organizzativo privacy dell'Università degli Studi di Pavia" adottato con determinazione n. 1909/2020 prot. n. 73471 del m10/7/2020;
- CONSIDERATE le proprie peculiarità organizzative, l'estensione e la dislocazione territoriale delle strutture universitarie e le caratteristiche degli edifici, al fine di migliorare la sicurezza e l'incolumità della comunità accademica, la tutela del patrimonio dell'Ateneo a fronte di un'esigenza effettiva e proporzionata di prevenzione di pericoli concreti e specifici di lesione di beni, e garantire un livello elevato di tutela dei diritti e delle libertà fondamentali;

- RITENUTO fondamentale definire le condizioni e le modalità di corretto utilizzo dei sistemi di videosorveglianza esistenti all'interno della proprietà universitaria

DISPONE

Art.1- di emanare il "Disciplinare su impiego di sistemi di videosorveglianza negli ambienti dell'Università degli Studi di Pavia ' di cui all'allegato 1, che costituisce parte integrante del presente provvedimento.

IL DIRETTORE GENERALE

Dott.ssa Emma Varasio

(Documento firmato digitalmente)

DISCIPLINARE SULL'IMPIEGO DI SISTEMI DI VIDEOSORVEGLIANZA NEGLI AMBIENTI DELL'UNIVERSITÀ DEGLI STUDI DI PAVIA

Sommario

1. Introduzione

La sorveglianza sistematica e automatizzata di uno spazio specifico con mezzi ottici o audiovisivi è l'attività che comporta la raccolta e la conservazione di immagini e informazioni grafiche o audiovisive su tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici. L'identità di tali persone può essere stabilita sulla base delle informazioni così raccolte.

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali. L'attività di videosorveglianza e di registrazione delle immagini deve essere svolta nell'osservanza della normativa vigente, per evitare di incorrere in un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati e tutelando la dignità delle persone riprese. Nel gestire la videosorveglianza occorre osservare sempre attentamente i principi generali del Regolamento Generale sulla Protezione dei Dati, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 - RGPD.

Il presente disciplinare è finalizzato a fornire indicazioni sull'applicazione del RGPD in relazione al trattamento di dati personali attraverso dispositivi video al fine di garantire il rispetto della normativa.

2. Ambito di applicazione

Il presente disciplinare non si applica al trattamento di dati che non hanno alcun riferimento a una persona, ad esempio se una persona non può essere identificata, direttamente o indirettamente.

3. Definizioni

Ai fini del seguente documento si definisce:

a) "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;
b) "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;
c) "Titolare": l'Università degli Studi di Pavia, nella persona del Magnifico Rettore, cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento di dati personali;
d) "Responsabili interni designati", soggetti, espressamente designati dal Titolare sulla scorta del proprio assetto organizzativo, a cui sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle norme in materia di protezione dei dati (es: Dirigenti, Direttori Dipartimento);

e) "Responsabile esterno 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 quale l'azienda che fornisce supporto e manutenzione (art. 28 RGPD);
f) "Incaricato/Autorizzato", le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
g) " Interessato", la persona fisica cui si riferiscono i dati personali;
h) "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;
i) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
j) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
k) "violazione dei dati personali": la violazione di tipo accidentale o illecito dei dati personali che può consistere nella distruzione, nella perdita, nella modifica, nella divulgazione non autorizzata o nell'accesso ai dati personali trasmessi, conservati o comunque trattati;
l) "RGPD", il Regolamento Generale sulla Protezione dei Dati, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
m) "Codice", il D. Lgs. n. 196/2003, recante Codice in materia di protezione dei dati personali, come aggiornato dal D.Lgs 10 agosto 2018, n. 101;
n) "Garante", il Garante per la protezione dei dati personali di cui all'art. 153 del Codice;
o) "Provvedimento Generale", il Provvedimento in materia di videosorveglianza emanato dal Garante in data 08/ 04/2010.
p) "Amministratore di sistema" in ambito informatico: figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento del *Garante Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* (G.U. n. 300 del 24 dicembre 2008 modificato in base al provvedimento del 25 giugno 2009) vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
q) "terzo" 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

4. Liceità del trattamento e finalità

Prima di attivare la videosorveglianza, si devono specificare dettagliatamente le finalità del trattamento (articolo 5, paragrafo 1, lettera b) RGPD). Queste finalità del monitoraggio devono essere documentate per iscritto e devono essere specificate per ogni sistema di rilevazione delle immagini in uso. Le telecamere utilizzate per lo stesso scopo da un unico Titolare del trattamento possono essere oggetto di una documentazione unitaria. Gli interessati devono essere informati delle finalità del trattamento.

4.1 Finalità

L'installazione di sistemi di rilevazione delle immagini da parte dell'Università rinviene la sua legittimazione nello svolgimento di funzioni istituzionali, di cui è Titolare in base all'ordinamento di riferimento. Il trattamento dei dati personali, effettuato mediante l'istallazione di sistemi di

rilevazione delle immagini all'interno delle strutture universitarie, risponde alle seguenti finalità determinate, esplicite e legittime:

- aumentare la sicurezza e incolumità del personale universitario, degli studenti e dei frequentatori a vario titolo degli spazi universitari;

- tutelare il patrimonio mobiliare e immobiliare dell'Ateneo;

- prevenire atti vandalici in assenza di altri strumenti idonei;

L'Università assicura che le immagini non siano in alcun modo impiegate come strumento di sorveglianza a distanza dei docenti, del personale tecnico – amministrativo e CEL, degli studenti e degli altri utenti dell'Università.

I dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nel presente disciplinare.

4.2 Necessità del trattamento

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati») limitando l'angolo visuale delle riprese e la conservazione.

I sistemi informativi e di programmi informatici devono essere configurati al fine di ridurre al minimo l'utilizzazione di dati personali.

Le varie fasi del trattamento sono definite in modo da comportare un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite.

Prima di installare un sistema di videosorveglianza, occorre sempre valutare se questa misura sia in primo luogo idonea a raggiungere l'obiettivo desiderato e, in secondo luogo, adeguata, necessaria e indispensabile per raggiungere lo scopo che ci si prefigge. Le misure di videosorveglianza possono essere adottate unicamente se la finalità del trattamento non possono ragionevolmente essere raggiunte con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato, quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, una migliore illuminazione~~,~~ abilitazioni agli ingressi.

5. Modello Organizzativo

5.1 Responsabilità

L'Università degli Studi di Pavia, nella persona del Rettore pro tempore, è Titolare dei trattamenti di dati personali effettuati mediante sistemi di videosorveglianza effettuati presso l'Università.

Il Titolare cura i rapporti con il Garante.

In particolare l'Università, 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, richiede la verifica preliminare del Garante in ordine alla legittimità del trattamento.

L'Università ha individuato i Responsabili interni del trattamento (Designati), quali soggetti

appositamente designati sulla scorta del proprio assetto organizzativo, conformemente a quanto previsto dal Codice in materia di protezione dei dati personali. I Responsabili interni al trattamento sono stati individuati nelle seguenti funzioni:

- Il Direttore Generale
- I Dirigenti d'Area;
- I Direttori di Dipartimento
- I Direttori dei Centri di servizio
- I Presidenti delle Scuole di Specializzazione
- Il Presidente della Commissione Servizio ispettivo
- I Responsabili di altre tipologie di strutture

I Responsabili interni, ciascuno per la propria area di competenza, garantiscono, insieme al Titolare, l'osservanza della normativa europea in tema di protezione dei dati personali. Al Responsabile interno sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle nuove norme in materia di privacy.

5.2 Gestione operativa sistemi videosorveglianza

Il Responsabile designato è tenuto a:

a) predisporre, aggiornare e conservare agli atti una documentazione delle scelte, in cui vengono adeguatamente spiegate le ragioni del ricorso alla videosorveglianza;
b) inserire e aggiornare il trattamento nel registro dei trattamenti d'Ateneo;
c) acquisire dall'installatore la dichiarazione che l'impianto è conforme alle norme previste dal RGPD, dal Codice e dalla normativa;
d) perfezionare l'accordo di designazione a responsabile esterno al trattamento del fornitore del servizio qualora ne ricorrano i presupposti;
e) individuare i soggetti autorizzati a compiere operazioni di trattamento e definire i profili di abilitazione per l'accesso alle immagini (preposti ad utilizzare gli impianti, visualizzare le immagini, ad accedere ai locali dove si trovano le postazioni di controllo e ad effettuare eventuali ulteriori operazioni) fornendo agli stessi istruzioni per il corretto trattamento dei dati, fermo restando l'accesso consentito alla polizia giudiziaria, nei casi espressamente previsti per motivi di ordine pubblico, sicurezza, tutela del patrimonio e repressione dei reati;
f) vigilare sulla conservazione delle immagini e sulla loro cancellazione nei termini previsti dal presente Regolamento;
g) riesaminare in differita le immagini in caso di effettiva necessità, per il conseguimento delle finalità indicate all'art. 4 del presente Disciplinare;
h) vigilare sulla manutenzione ordinaria e straordinaria dei sistemi, garantendo l'osservanza della normativa vigente e del presente disciplinare da parte di chi entri in contatto con i dati registrati;
i) monitorare periodicamente gli impianti di videosorveglianza per verificare le misure per garantire la sicurezza dei dati
j) provvedere in ordine all'installazione della segnaletica in prossimità dell'impianto di videosorveglianza;
k) presidiare il monitoraggio dell'informativa semplificata tramite cartellonistica e dell'informativa per esteso;
l) garantire l'esercizio dei diritti degli interessati predisponendo ogni adempimento organizzativo

necessario;

m) individuare e designare una o più persone di riferimento (*Referenti Privacy*) che avranno il compito di supporto per gli adempimenti previsti dalla normativa vigente;
n) designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
o) raccogliere ogni segnalazione di violazione di dati personali da parte di dipendenti, collaboratori e/o interessati e comunicarla tempestivamente al Responsabile della Protezione dei Dati e al Titolare secondo la procedura di segnalazione della violazione di dati personali (data breach) adottata dall'Ateneo;
p) effettuare preventiva valutazione d'impatto nei casi previsti secondo la procedura adottata dall'Ateneo e, ove i risultati della valutazione d'impatto sulla protezione dei dati indichino che il trattamento comporterebbe un rischio elevato nonostante le misure di sicurezza pianificate, informare il Titolare;
q) In caso di dismissione dell'impianto per motivi di costi, obsolescenza e sicurezza attivare tutte le procedure tecniche per la cancellazione sicura dei dati e relative copie nella disponibilità dell'ente.

6. Modalità di esecuzione dell'attività di videosorveglianza: la documentazione delle scelte

Il Responsabile interno designato è tenuto a compilare e conservare agli atti la scheda relativa alla documentazione delle scelte, resa disponibile dall'Ateneo, con le caratteristiche tecniche della videosorveglianza, unitamente agli allegati in essa richiesti o menzionati, la quale, altresì, rappresenta una documentazione necessaria per la manutenzione del servizio stesso, per il registro dei trattamenti e per la fase istruttoria richiesta dagli artt. 33 e 34 del RGPD, nella eventuale situazione di violazione dei dati personali (data breach).

Più precisamente, nella scheda dovranno essere indicate:

- la mappatura per le varie sedi dei sistemi di videosorveglianza, con le relative specifiche tecniche, al fine di verificare la conformità degli strumenti utilizzati ai principi dedotti nel presente Disciplinare;
- le specifiche tecniche del sistema di conservazione delle immagini;
- le specifiche tecniche delle misure di sicurezza adottate.

Le immagini sono conservate nel rispetto delle misure di sicurezza richieste dalla normativa vigente e delle policies di sicurezza informatica definite per i sistemi informativi. Il trattamento dei dati personali, effettuato mediante l'installazione degli impianti di videosorveglianza, deve essere attuato nel rispetto dei principi generali, specificati all'art. 4 del presente documento.

Le videocamere che verranno installate non potranno mai essere orientate sui terminali di rilevazione presenza né sulle postazioni di lavoro.

Laddove dai sistemi installati per le finalità sopra elencate derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, l'Ateneo adotta le garanzie previste dall'art. 4, comma 2, della l. n. 300/1970, sottoponendo in via preventiva il progetto di installazione dei sistemi alle rappresentanze sindacali aziendali e, in mancanza di raggiungimento di un accordo, presentando istanza all'Ispettorato del lavoro.

La dislocazione delle videocamere e le modalità di ripresa sarà predisposta a seguito di attenta e ponderata valutazione, in modo da non interferire con le attività di studio-lavoro-ricerca. Le telecamere poste all'interno delle aule, sono rese operative unicamente negli orari preventivamente stabiliti.

Il Titolare del trattamento, ai sensi dell'art. 35 del Regolamento UE 2016/679, è tenuto a condurre una valutazione d'impatto sulla protezione dati qualora i trattamenti, allorché prevedano in particolare l'uso di nuove tecnologie, che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

7. Conservazione e obbligo di cancellazione dei dati

1. I dati personali non possono essere conservati più a lungo di quanto necessario per le finalità di trattamento.
2. La necessità di conservare i dati personali deve essere valutata entro una tempistica ristretta. In relazione alle finalità perseguite occorre valutare se sia più opportuno conservare e cancellare automaticamente le registrazioni dopo un lasso di tempo oppure ricorrere al monitoraggio in tempo reale senza registrazione.
3. La conservazione è limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, in ogni caso non oltre il tempo massimo di cinque giorni dalla rilevazione, salvo il caso in cui sussista la necessità di aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o della polizia giudiziaria. Se la videosorveglianza serve allo scopo di rilevare il compimento di eventuali atti vandalici, la protezione del patrimonio o la conservazione di elementi di prova, solitamente è possibile individuare eventuali danni entro le successive quarantotto ore, tenendo conto dei principi di cui all'articolo 5, paragrafo 1, lettere c) ed e), del RGPD, vale a dire la minimizzazione dei dati e la limitazione della loro conservazione. I dati personali devono essere cancellati entro i successivi cinque giorni lavorativi.
4. La conservazione, per un periodo di tempo superiore alla settimana, necessita di un'attenta e motivata analisi riferita alla legittimità dello scopo e alla necessità della conservazione, oltre alla verifica preliminare del Garante. da richiedere a cura del Titolare.
5. Il sistema impiegato deve essere programmato al fine di cancellare automaticamente, alla scadenza del termine di conservazione, le immagini registrate da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

8. Misure tecniche di sicurezza

Il Titolare del trattamento dei dati adotta le misure idonee e preventive di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità di raccolta, anche in relazione alla trasmissione delle immagini e alla loro conservazione entro i tempi individuati. In particolare, a norma degli artt. 24 e25 del RGPD, sono adottate specifiche misure tecniche ed organizzative proporzionate ai rischi per i diritti e le libertà delle persone fisiche, al fine di salvaguardare tutti i principi di protezione dei dati durante il trattamento e stabilire i mezzi affinché gli interessati possano esercitare i propri diritti.

Un sistema di videosorveglianza (VSS) è costituito da dispositivi analogici e digitali nonché da software per acquisire immagini, gestirle e mostrarle a un operatore.

La sicurezza di un VSS consiste nella riservatezza, nell'integrità e nella disponibilità del sistema e dei dati:

- la sicurezza del sistema comprende la sicurezza fisica di tutti i componenti del sistema, comprese le reti di trasmissione dati a cui il dispositivo è eventualmente collegato e il controllo dell'accesso anche da remoto al VSS,
- la sicurezza dei dati comprende la prevenzione della perdita o della manipolazione dei dati.

Dal punto di vista tecnico, le specifiche e la progettazione del sistema devono includere requisiti per il trattamento dei dati personali conformemente ai principi di cui all'articolo 5 del RGPD (liceità del trattamento, limitazione della finalità e dei dati, minimizzazione dei dati per impostazione predefinita ai sensi dell'articolo 25, paragrafo 2, del RGPD, integrità e riservatezza, responsabilizzazione, ecc.).

In fase di acquisizione di un sistema di videosorveglianza occorre verificare che vengano fornite le specifiche attestazioni e certificazioni tecniche, nel rispetto dei principi privacy by default e privacy by design in conformità al RGPD. Il Titolare del trattamento deve garantire la conformità a questi requisiti, applicandoli a tutti i componenti del sistema e a tutti i dati da esso trattati, durante l'intero ciclo di vita.

Tutti i componenti di un sistema di videosorveglianza e i dati acquisiti devono essere adeguatamente protetti durante:

- la conservazione (dati a riposo);
- la trasmissione (dati in transito);
- il trattamento (dati in uso).

A tal fine è necessario combinare le misure organizzative indicate all'articolo 5 del presente Disciplinare e le misure tecniche.

Nel selezionare le soluzioni tecniche, occorre considerare le tecnologie che tutelano la privacy anche perché migliorano la sicurezza. Esempi di questo tipo di tecnologie sono i sistemi che consentono il mascheramento o l'offuscamento delle zone irrilevanti per la sorveglianza, oppure l'editing di immagini di terzi, quando si forniscono filmati agli interessati in risposta alle richieste di accesso.

Le soluzioni individuate non devono prevedere funzioni non necessarie (ad esempio, movimento illimitato delle telecamere, capacità di zoom, radiotrasmissione, analisi e registrazioni audio). Le funzioni fornite, ma non necessarie, devono essere disattivate.

Deve essere consentito al titolare di verificare l´attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa, alla luce anche di quanto previsto in merito al controllo sull'operato degli amministratori di sistema.

I dati raccolti mediante i sistemi di videosorveglianza sono protetti, ai sensi dell'art. 32 del RGPD, con misure tecniche e organizzative adeguate, 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. Gli apparati di ripresa digitali connessi a reti informatiche sono protetti contro i rischi di accesso abusivo di cui all'art. 615 ter del codice penale.

9. Comunicazione di filmati a terzi

Qualsiasi comunicazione di dati personali costituisce uno specifico trattamento per l'effettuazione del quale il Titolare deve trovare legittimazione tra le previsioni dell'articolo 6 del RGPD.

La comunicazione a soggetti pubblici dei dati personali, acquisiti mediante i sistemi di videosorveglianza, è ammessa solo se prevista da disposizioni di legge, fatti salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico, oppure, in mancanza, quando è necessaria per lo svolgimento delle funzioni istituzionali dell'Università, sempre in conformità ai principi di necessità e proporzionalità, sentito il Responsabile per la protezione dei dati personali.

Sono fatte salve, in ogni caso, la comunicazione di dati richiesti, in conformità alla legge, dalle forze dell'ordine, dall'autorità giudiziaria o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del Codice per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Il trattamento dei dati personali da parte delle autorità di contrasto non è disciplinato dal RGPD, bensì dalla direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie.

La comunicazione e la diffusione devono essere, in ogni caso, autorizzate dal Titolare del trattamento.

10. Diritti dell'interessato

Data la natura del trattamento dei dati associato all'impiego della videosorveglianza, agli interessati identificati o facilmente identificabili è riconosciuto l'effettivo esercizio dei propri diritti in conformità al Regolamento (UE) 2016/679, così come definiti all'art. 2, in conformità agli artt. 15, 17, 18, 19 e 21 del RGPD e il Diritto di reclamo ad un'autorità di controllo (art. 77).

In taluni casi le azioni di cancellazione e di opposizione al trattamento, ai sensi dell'art.21 del RGPD, non sono consentite. In particolare, esistono alcune limitazioni che possono trovare applicazione rispetto al diritto di accesso, tra cui la lesione dei diritti altrui e quando non è sia possibile identificare l'interessato.

Nella sua richiesta scritta e motivata per la tutela di situazioni giuridicamente rilevanti al Titolare del trattamento o al Responsabile interno designato anche tramite il Responsabile Protezione Dati, l'interessato, oltre a identificarsi mediante presentazione di un documento d'identità o di persona, deve specificare quando – entro un lasso di tempo ragionevole in proporzione alla quantità di interessati registrati – è entrato nella zona sorvegliata.

Le richieste devono essere protocollate ed inserite nel registro degli accessi dai referenti privacy tramite la procedura DPM. Se il Titolare del trattamento può dimostrare di non essere in grado di identificare l'interessato, ne informa quest'ultimo. Il diritto di accesso da parte dell'interessato alle

immagini acquisite mediante i sistemi di videosorveglianza e conservate presso l'Università degli Studi di Pavia è disciplinato, rispettivamente, dal RGPD, dal Codice o dalla L. n. 241/1990.

In caso di richieste eccessivamente gravose o manifestamente infondate, il Titolare del trattamento può addebitare al richiedente un contributo spese ragionevole o rifiutarsi di dare seguito alla richiesta dimostrando il carattere manifestamente infondato o eccessivo della richiesta.

11. Obblighi di trasparenza e informativa agli interessati

L'Università informa gli interessati in ordine alla presenza negli spazi universitari di sistemi di videosorveglianza mediante l'affissione nelle zone interessate, in prossimità della videocamera, del modello di informativa (All. n. 1), indicante il Titolare del trattamento e le finalità perseguite.

L'informativa è collocata prima del raggio di azione della videocamera, in posizione che ne garantisca la visibilità in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza è attivo in orario notturno.

In presenza di più videocamere e in relazione alla vastità delle aree oggetto di rilevamento, l'informativa è resa mediante affissione di una pluralità di cartelli.

L'Università mette a disposizione degli interessati sul proprio sito internet e con ogni ulteriore mezzo di pubblicità ritenuto idoneo, presso le sedi dell'Ateneo, il testo completo dell'informativa, contenente tutti gli elementi di cui all' art. 13, Regolamento (UE) 2016/679 (All. n. 2).

ALLEGATI

ALL. n. 1 informativa semplificata

ALL. n. 2 informativa completa

UNIVERSITÀ DI PAVIA

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI ACQUISITI TRAMITE I SISTEMI DI VIDEOSORVEGLIANZA INSTALLATI PRESSO LE STRUTTURE DELL'UNIVERSITA' DEGLI STUDI DI PAVIA

ai sensi dell'art. 13 e 14 del Regolamento (UE) 2016/679 -RGPD

Titolare del trattamento

Il Titolare del trattamento è l'Università degli Studi di Pavia, nella persona del Magnifico Rettore (sede C.so Strada Nuova n. 65, 27100 Pavia, PEC amministrazione-centrale@certunipv.it). L'Università degli Studi di Pavia ha nominato il Responsabile della Protezione Dati RPD. I dati di contatto sono: Università degli Studi di Pavia, C.so Strada Nuova n. 65, 27100 Pavia, Email: privacy@unipv.it PEC amministrazione-centrale@certunipv.it

Il Responsabile interno designato al trattamento dati varia in base alla sede di installazione dell'impianto ed è riportato nell'informativa semplificata esposta in corrispondenza dell'area videosorvegliata

Finalità del trattamento – base giuridica:

I dati personali saranno trattati dall'Università per il perseguimento delle proprie finalità istituzionali nel rispetto dei principi di liceità, correttezza, trasparenza, adeguatezza, pertinenza e necessità di cui all'art. 5, paragrafo 1, del RGPD.

Il trattamento dei dati personali, raccolti tramite i sistemi di videosorveglianza, è finalizzato esclusivamente per favorire la sicurezza e l'incolumità del personale universitario, degli studenti e dei frequentatori a vario titolo degli spazi e dei locali universitari; salvaguardare il patrimonio mobiliare e immobiliare dell'Ateneo; prevenire atti vandalici in assenza di altri strumenti idonei.

Il trattamento è effettuato dall'Università degli Studi di Pavia ha ad oggetto le immagini delle persone che si trovano a transitare nel raggio d'azione di tali sistemi.

L'attività viene svolta nel rispetto del *Disciplinare sull'impiego di sistemi di videosorveglianza negli ambienti dell'Università degli Studi di Pavia* pubblicato all'indirizzo: https://web.unipv.it/ateneo/statuto-regolamenti/

I dati saranno trattati mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi in conformità alle norme vigenti e non verranno in alcun modo utilizzati per tracciare profili di preferenza degli studenti (compresa la profilazione).

Natura del conferimento dei dati e conseguenza del rifiuto

Gli interessati vengono preventivamente informati che stanno per accedere ad una zona sottoposta a videosorveglianza; essendo strettamente strumentale all'accesso a tali spazi, il conferimento dei dati è obbligatorio.

Categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati – Destinatari dei dati

I dati personali degli utenti potranno essere conosciuti e trattati, nel rispetto della vigente normativa in materia, da personale e da collaboratori dei competenti uffici dell'Università, autorizzati e adeguatamente istruiti dal Titolare, o dai fornitori di servizi espressamente nominati come responsabili esterni del trattamento (a norma dell'art. 28 del RGPD). In alcuni casi le immagini possono essere solo registrate, in altre anche rilevate da personale opportunamente autorizzato e istruito al trattamento.

I dati potranno essere trasmessi all'Autorità giudiziaria nei casi previsti dalla legge.

Non è previsto il trasferimento dei dati personali verso destinatari in Stati extra-UE o verso organizzazioni internazionali.
Non è prevista attività di profilazione.

Conservazione

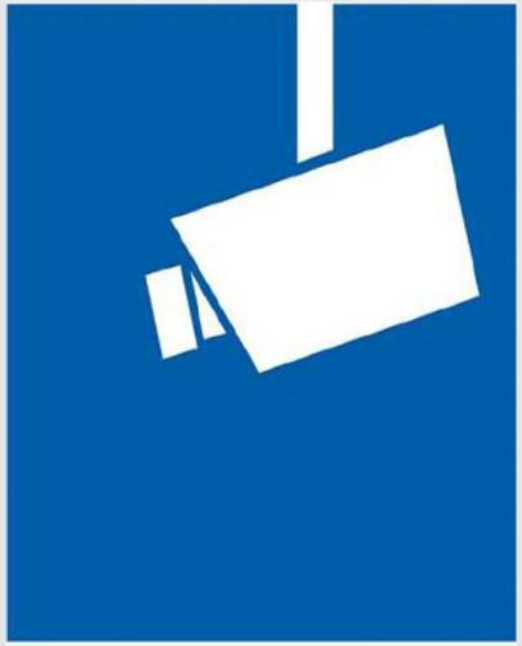
Le immagini registrate sono conservate esclusivamente per il tempo necessario a raggiungere le finalità perseguite e, in ogni caso, non oltre il tempo massimo di 5 giorni, fatti salvi il caso di specifica richiesta di soggetti pubblici legittimati e il caso di periodi di chiusura programmata e prolungata dell'Ateneo e comunque non oltre la settimana. Decorso il termine, le immagini vengono cancellate.

Diritti dell'Interessato

Gli interessati possono esercitare i diritti sui dati previsti dagli artt. 15-21 del Regolamento (UE) 2016/679. L'apposita istanza è presentata al Titolare e/o il RPD, ovvero il Responsabile interno del trattamento, anche tramite e-mail. Gli interessati, ricorrendone i presupposti, hanno inoltre il diritto di proporre reclamo all'autorità di controllo Garante per la protezione dei dati personali secondo le procedure previste dal Regolamento (UE) 2016/679.

MODELLO SEMPLIFICATO CARTELLO VIDEOSORVEGLIANZA

(EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020)



LA REGISTRAZIONE È EFFETTUATA DALL' UNIVERSITA' DEGLI STUDI DI PAVIA
sede C.so Strada Nuova n. 65, 27100 Pavia, PEC amministrazione-centrale@certunipv.it

CONTATTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD): privacy@unipv.it

RESPONSABILE INTERNO DESIGNATO: (specificare Dirigente/Direttore di Dip. …)

LE IMMAGINI SARANNO CONSERVATE PER UN PERIODO DI
(riportare quanto indicato nella "documentazione delle scelte")

FINALITÀ DELLA VIDEOSORVEGLIANZA:
- aumentare la sicurezza;
- tutelare il patrimonio mobiliare e immobiliare dell'Ateneo;
- prevenire atti vandalici in assenza di altri strumenti idonei.

L'informativa completa sul trattamento dei dati è disponibile:

- **sul sito internet https://privacy.unipv.it**

È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI:
all'UNIVERSITA' DEGLI STUDI DI PAVIA e/o
al RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)
ovvero al RESPONSABILE INTERNO DESIGNATO.