UNIVERSITÀ DEGLI STUDI FIRENZE

Area Affari Generali e Legali

LA RETTRICE

VISTO il vigente Statuto dell'Università degli Studi di Firenze emanato con Decreto rettorale 30 novembre 2018, n. 1680 – prot. n. 207006;

VISTO il vigente Regolamento di Amministrazione, Finanza e Contabilità dell'Università degli Studi di Firenze emanato con Decreto rettorale 8 maggio 2014, n. 405 - prot. n. 35026;

VISTO il Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, entrato in vigore il 25 maggio 2016, che abroga la direttiva 95/46/CE ed è direttamente applicabile e vincolante in tutti gli Stati membri e non richiede una legge di recepimento nazionale (Regolamento Generale sulla Protezione dei Dati);

VISTA la Legge 25 ottobre 2017, n. 163 di delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento suddetto;

VISTO il Decreto Legislativo 10 agosto 2018, n. 101 recante 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;

VISTO il Decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali e s.m.i;

PREMESSO CHE nel contesto attuale nell'Università degli Studi di Firenze due sono gli atti che disciplinano la materia della videosorveglianza**:**

1. L'Accordo relativo all'installazione ed utilizzo del sistema di videosorveglianza ai sensi dell'art. 4 della legge n. 300/1970 del 6 luglio 2022
2. il "Regolamento per la disciplina dell'utilizzo e la gestione dei sistemi di videosorveglianza presenti nel Polo delle Scienze Sociali" (Decreto rettorale, 3 luglio 2006, n. 536 prot. n. 35856**;**

PREMESSO CHE sono state riscontrate delle criticità correlate all'entrata in vigore Regolamento Generale sulla Protezione dei Dati (Reg. UE n. 679/2016) in materia di protezione dei dati che potrebbero esporre l'Università a rischi di sanzioni da parte del Garante per la protezione dei dati personali per inadempimento degli obblighi previsti dalla normativa in materia di protezione dei dati, soprattutto per l'incertezza relativa a diversi fattori quali**:**

- modalità e tempi di conservazione dei dati;
- procedure di raccolta;
- segnaletica non conforme alla nuova normativa;
- ruoli dei diversi attori che intervengono nelle attività di trattamento;

PREMESSO CHE è emersa la necessità di aumentare i tempi di conservazione delle registrazioni del sistema di videosorveglianza sia per garantire una maggior sicurezza della comunità universitaria e degli ambienti di Ateneo sia per la prevenzione o la eventuale persecuzione di reati;

PRESO ATTO delle indicazioni fornite dal Comitato Europeo per la Protezione dei Dati (European Data Protection Board - EDPB) che il 29 gennaio 2020 ha adottato la versione definitiva delle linee guida sui trattamenti di videosorveglianza – Guidelines 3⁄2019 on processing of personal data through video devices – che chiariscono in quali termini il Regolamento 2016⁄679 UE (GDPR) si applichi al trattamento dei dati personali mediante dispositivi video e anche di raccolta di immagini fotografiche;

RITENUTA OPPORTUNA l'adozione di un nuovo regolamento in materia di videosorveglianza che:
- sia aggiornato al nuovo contesto normativo;
- recepisca le indicazioni fornite nel nuovo Accordo relativo all'installazione ed utilizzo del sistema di videosorveglianza;
- disciplini alcuni ambiti che sono da ritenere essenziali alla fine del trattamento dei dati quali:
- chiarire le finalità del trattamento;
- individuare i soggetti autorizzati al trattamento e definire i loro ruoli;
- informare sui metodi di raccolta e conservazione dei dati;
- delimitare i tempi di conservazione dei dati;
- prevedere l'adozione di misure di sicurezza adeguate;
- indicare come adempiere agli obblighi informativi di cui all'art. 13 del GDPR;
- prevedere come garantire i diritti degli interessati previsti dalla normativa;
- indicare eventuali obblighi di comunicazione ad altri soggetti e se del caso stabilire le modalità per tali comunicazioni;
- informare di eventuali trasferimenti dei dati verso Paesi Terzi

VISTA la proposta di *Regolamento in materia di Videosorveglianza dell'Università degli Studi di Firenze*;

ACQUISITO il parere del Comitato Tecnico amministrativo espresso nella seduta del 10 gennaio 2022;

VISTO il parere favorevole della Commissione Affari Generali e Normativi espresso nella seduta del 13 gennaio 2022;

VISTA la delibera del Consiglio di amministrazione del 28 luglio 2022;

UNIVERSITÀ DEGLI STUDI FIRENZE

VISTO il parere del Senato Accademico espresso nella seduta del 21 settembre 2022,

DECRETA

per le finalità di cui in premessa è emanato il *Regolamento in materia di videosorveglianza dell'Università degli Studi di Firenze* nel seguente testo, che abroga e sostituisce il "Regolamento per la disciplina dell'utilizzo e la gestione dei sistemi di videosorveglianza presenti nel Polo delle Scienze Sociali", di cui al Decreto rettorale, 3 luglio 2006, n. 536 prot. n. 35856.

REGOLAMENTO IN MATERIA DI VIDEOSORVEGLIANZA DELL'UNIVERSITÀ DEGLI STUDI DI FIRENZE

Sommario

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Art. 1 Definizioni

1. Ai fini del presente Regolamento si intende:

a) per “RGPD” il 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)”;

b) per “Statuto dei lavoratori” la Legge 20 maggio 1970, n. 300 “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento”;

c) per “titolare del trattamento” l’Università degli Studi di Firenze nella persona del Rettore in quanto soggetto che determina le finalità e i mezzi del trattamento di dati personali;

d) per “responsabile del trattamento” la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta i dati personali per conto del titolare del trattamento;

e) per “responsabile per la protezione dei dati” la persona designata all’interno dell’organizzazione ai sensi dell’art. 37 del RGPD con funzioni di consulenza e sorveglianza in merito alla normativa in materia di protezione dei dati;

f) per “soggetti autorizzati” le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;

g) per “persone designate” le persone fisiche espressamente designate dal titolare del trattamento che operano sotto la sua autorità cui sono attribuiti specifici compiti e funzioni connessi al trattamento di dati personali ai sensi dell’art. 2-quaterdecies del D.lgs. 30 giugno 2003, n. 196 e ss.mm.ii;

h) per “dato personale” qualsiasi informazione riguardante una 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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

i) per “dato anonimo” il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

j) per “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;

k) per “sistema di videosorveglianza” un sistema costituito da dispositivi analogici e digitali quali unità di ripresa, apparati di trasmissione, di comando, di illuminazione, di visione e di videoregistrazione, nonché da software per acquisire e registrare immagini, gestirle, mostrarle a un operatore;

l) per “archivio” qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

m) per "interessato" la persona fisica identificata o identificabile attraverso i dati personali;

n) per “misure di sicurezza” il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello di protezione idoneo a garantire un livello di sicurezza adeguato al rischio derivante dalle attività di trattamento;

o) per “comunicazione” la trasmissione dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione Europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

p) per “diffusione” la trasmissione dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 2 Principi generali

1. La raccolta, la rilevazione, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configurano un trattamento di dati personali ai sensi dell’art. 4 del RGPD.

2. Il trattamento dei dati personali effettuato mediante l’attivazione di impianti di videosorveglianza si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, garantendo la riservatezza, l’identità personale e i diritti degli interessati coinvolti nel trattamento.

3. La determinazione della dislocazione delle videocamere e delle modalità di ripresa e il trattamento dei dati raccolti vengono effettuati nel rispetto dei principi di cui all’art 5 del RGPD e in particolare:

- principio di liceità: il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- principio di necessità: il sistema di videosorveglianza, i sistemi informativi e i programmi informatici utilizzati sono configurati per ridurre al minimo l'utilizzazione di dati personali in modo da escluderne il trattamento quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi o con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato;
- principio di proporzionalità: nell'attività di videosorveglianza, nella scelta delle modalità di ripresa e di dislocazione, nonché nelle varie fasi del trattamento i dati trattati devono comunque essere pertinenti e non eccedenti rispetto alle finalità perseguite;
- principio di correttezza e trasparenza: l'interessato deve essere informato del trattamento dei propri dati personali effettuato tramite il sistema di videosorveglianza e delle relative finalità perseguite dall'Università.

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 a fare una valutazione di impatto del trattamento ai sensi dell'art. 35 RGPD. A tal fine si consulta con il RPD e, a seconda degli esiti, prima di procedere al trattamento consulta l'autorità garante, secondo quanto previsto all'art. 36 RGPD.

5. Quando dall'installazione di impianti di videosorveglianza in ambienti lavorativi chiusi e dedicati esclusivamente ai lavoratori deriva anche la possibilità di controllo a distanza dell'attività dei lavoratori, gli impianti possono essere installati soltanto previo accordo con le rappresentanze sindacali di Ateneo, ai sensi dell'art. 4 dello Statuto dei lavoratori. In mancanza di accordo il sistema di videosorveglianza può essere installato previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro.

Art. 3 Finalità

1. Il presente Regolamento disciplina il funzionamento dei sistemi di videosorveglianza installati presso le strutture dell'Università degli Studi di Firenze e il trattamento dei dati personali registrati.

2. Il trattamento di dati personali attraverso sistemi di videosorveglianza da parte dell'Università avviene esclusivamente nell'ambito dello svolgimento delle funzioni istituzionali, e comunque al fine di favorire la prevenzione di eventi dannosi a seguito di furti, atti vandalici, azioni lesive del patrimonio dell'Ateneo e garantire la sicurezza di tutta la comunità universitaria, nonché per la verifica della funzionalità degli impianti e per la protezione dei beni artistici e dei valori museali.

3. L'installazione di sistemi di rilevazione delle immagini da parte dell'Università risponde alle seguenti finalità, determinate, esplicite e legittime:

a) favorire un adeguato grado di sicurezza a tutta la popolazione universitaria;
b) tutelare gli immobili in gestione dell'amministrazione universitaria;
c) tutelare i beni mobili presenti nelle sedi universitarie.

4. Si provvede alla raccolta dei dati strettamente necessari per il raggiungimento delle finalità sopra elencate, 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 degli enti locali.

Art. 4 Soggetti

1. Al titolare del trattamento compete ogni decisione in ordine alle finalità e ai mezzi di trattamento dei dati personali, compresa l'individuazione degli strumenti da utilizzare e delle misure di sicurezza da adottare.

2. Il titolare del trattamento ricorre a responsabili del trattamento dotati di adeguata competenza e in grado di mettere in atto misure tecniche e organizzative adeguate perla tutela dei diritti dell'interessato quando per la gestione del sistema di videosorveglianza, faccia ricorso a soggetti esterni ai quali affidare incarichi, servizi, lavori, forniture o consulenze che comportino un trattamento di dati per conto dell'Università. In questi casi, si procederà a disciplinare i trattamenti da parte del Responsabile mediante contratto ovvero altro atto giuridico che vincoli il responsabile del trattamento al titolare del trattamento ai sensi dell'art. 28, RGPD.

3. Il titolare del trattamento attribuisce, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, specifici compiti e funzioni connessi al trattamento di dati personali a persone fisiche, espressamente designate, che operano sotto la sua autorità. Potranno essere autorizzati al trattamento dei dati anche persone fisiche esterne all'organizzazione universitaria, che in adempimento a obblighi di natura contrattuale eseguono attività di trattamento sotto la diretta autorità del titolare.

4. I soggetti autorizzati ad utilizzare gli impianti e a visionare le registrazioni svolgono le operazioni materiali di trattamento attenendosi alle istruzioni impartite dal titolare del trattamento, che provvede ad aggiornarle in caso di modifiche organizzative, tecniche e normative.

Art. 5 Raccolta e trattamento dei dati

1. La raccolta dei dati avviene tramite videocamere aventi le caratteristiche tecniche descritte in un apposito documento conservato dal titolare del trattamento. Il titolare del trattamento modifica il documento nel rispetto di quanto previsto dal presente Regolamento e previa informazione alle OO.SS., alle RSU e agli Organi competenti in relazione ai mutamenti del quadro tecnologico o delle finalità dell'attività di video sorveglianza.

2. Le videocamere installate presso le sedi dell'Università consentono unicamente riprese video e non effettuano riprese audio. La registrazione delle immagini avviene con videocamere a immagine fissa. Le videocamere installate agli accessi dei plessi universitari non sono orientate sui lettori di badge, sulle postazioni di lavoro o su luoghi riservati esclusivamente al personale dipendente (spogliatoi o servizi).

3. Non sono installate apparecchiature specificatamente preordinate al controllo a distanza dell'attività del personale universitario e di tutti coloro che operano a vario titolo all'interno dei locali universitari, non sono effettuate riprese per 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. In caso di rilevazione di immagini o fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza, della tutela ambientale o del patrimonio pubblico, il titolare del trattamento provvede tempestivamente a darne comunicazione all'autorità competente, provvedendo alla conservazione delle immagini.

Art. 6 Conservazione e cancellazione dei dati

1. I dati raccolti durante l'orario di apertura degli edifici sottoposti a videosorveglianza sono visualizzati in tempo reale tramite i monitor collocati all'interno dei locali di portineria e sono conservati.

2. Le immagini registrate mediante le telecamere collocate presso le sedi universitarie sono conservate in appositi hard disk per un periodo non superiore alle 72 ore successive alla loro rilevazione. Un prolungamento del periodo di conservazione può essere autorizzato durante le festività o i periodi di chiusura delle sedi universitarie o su richiesta del titolare del trattamento o dell'autorità giudiziaria.

3. Per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio nei laboratori contenenti sostanze chimiche, radioattive, biologiche, negli stabulari), o per specifiche e motivate richieste da parte delle Strutture di Ateneo, con decreto del Rettore può essere consentito un periodo di conservazione dei dati più lungo non superiore alla settimana.

4. Le immagini registrate vengono cancellate automaticamente da ogni supporto allo scadere dei termini di conservazione stabiliti nel presente Regolamento, con sovra-registrazione e modalità che rendono inutilizzabili i dati cancellati; tale impostazione di cancellazione dei dati dai sistemi di registrazione non dovrà essere tecnicamente modificabile.

Art. 7 Misure di sicurezza

1. 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.

Dette misure assicurano:

a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento.

2. In particolare sono adottate le seguenti misure tecniche e organizzative:

a) nel caso di interventi derivanti da esigenze di manutenzione, i soggetti preposti accedono alle immagini solo se ciò è indispensabile al fine di effettuare eventuali verifiche tecniche, e in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini e per il solo tempo necessario all'intervento di manutenzione;
b) in presenza di differenti competenze specificatamente attribuite ai singoli operatori, sono configurati diversi livelli di visibilità e trattamento delle immagini;
c) se i sistemi sono configurati per la registrazione e la conservazione delle immagini, la visione delle immagini registrate e le operazioni di cancellazione o duplicazione sono autorizzate dal Rettore o da un suo delegato.

Il titolare vigila sulla condotta tenuta da chiunque abbia accesso ai dati personali trattati dall'Università; provvede ad istruire e formare gli incaricati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

Art. 8 Comunicazione e diffusione

1. La comunicazione a soggetti pubblici dei dati personali acquisiti mediante i sistemi di videosorveglianza è ammessa solo se prevista da norma 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 e il rispetto della normativa dell'Unione Europea in materia di riutilizzo delle informazioni del settore pubblico, oppure, in mancanza, quando è necessaria per lo svolgimento delle funzioni istituzionali dell'Università, in conformità ai principi di necessità e proporzionalità, sentito il Responsabile per la protezione dei dati personali.

2. Sono fatte salve in ogni caso la comunicazione e la diffusione dei dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D.Lgs. n. 196/2003 per finalità di difesa o di

sicurezza dello Stato o di prevenzione, accertamento o repressione di reati. I dati possono essere comunicati ad altre amministrazioni per finalità di sicurezza, controllo e allerta sanitarie.

3. La comunicazione è in ogni caso autorizzata dal titolare del trattamento.

4. Non è consentita la diffusione delle registrazioni acquisite mediante i sistemi di videosorveglianza.

Art. 9 Informativa agli interessati

1. L'Università degli Studi di Firenze, in ottemperanza agli obblighi imposti dal RGPD, informa gli interessati che stanno per accedere ad una zona sottoposta a videosorveglianza, mediante l'affissione nelle zone interessate, in prossimità della videocamera, di un cartello informativo (All. 1) che indica il titolare del trattamento, la finalità perseguita, il periodo di conservazione dei dati, le modalità di esercizio dei diritti riconosciuti dalla normativa in materia di protezione dei dati e dove poter reperire l'informativa completa.

2. Il cartello deve essere collocato prima del raggio di azione della videocamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; lo stesso per formato e posizionamento deve essere visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia attivo in orario notturno. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, sono installati più cartelli informativi.

3. 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.

Art. 10 Diritti degli interessati

1. L'interessato al trattamento esercita nei confronti del titolare del trattamento tutti i diritti previsti dagli articoli 15 e seguenti del RGPD e, in particolare, il diritto di accesso ai propri dati, il diritto di opposizione al trattamento, il diritto di limitazione del trattamento e il diritto alla cancellazione dei dati, nei limiti e alle condizioni stabilite dalla normativa vigente in materia.

2. Non è esercitabile il diritto alla portabilità dei dati di cui all'articolo 20 del Regolamento UE 2016/679 in quanto le immagini acquisite con il sistema di videosorveglianza non possono essere trasferite ad altri soggetti, salvo i casi di comunicazione a soggetti pubblici legittimati a richiedere i dati, come l'autorità giudiziaria e/o di pubblica sicurezza.

3. La risposta a una richiesta di accesso non comprende eventuali dati riferiti a terzi, a meno che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi al terzo. Non è possibile soddisfare la richiesta di accesso, decorsi i termini di conservazione sopra indicati.

4. Per esercitare i propri diritti, gli interessati si rivolgono al titolare del trattamento o al responsabile per la protezione dei dati, esibendo o allegando alla richiesta idonei documenti di riconoscimento. Il titolare fornisce una risposta entro un mese dalla richiesta, estensibile fino a tre mesi in caso di particolare complessità.

5. In caso di richieste eccessive o manifestamente infondate il titolare del trattamento può addebitare un contributo spese ragionevole a norma dell'articolo 12, paragrafo 5, lettera a), del RGPD, o rifiutarsi di dare seguito alla richiesta (articolo 12, paragrafo 5, lettera b), del RGPD).

Art. 11 Nuove attivazioni o revisioni dei sistemi di videosorveglianza

1. In caso di sopravvenute esigenze che rendono necessaria l'attivazione di nuovi sistemi di videosorveglianza o la sostituzione di quelli esistenti con impianti diversi, il titolare del trattamento, sentito il responsabile per la protezione dei dati, assicura il rispetto degli obblighi di cui all'art. 25 del RPGD inerenti la protezione dei dati fin dalla progettazione e l'attivazione delle misure di cui all'art. 2 c. 5 del presente Regolamento, nonché il rispetto delle previsioni di cui all'art. 4 dello Statuto dei Lavoratori.

Art. 12 Norma di rinvio

1. Per quanto non previsto dal presente Regolamento, si applicano le disposizioni previste dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, dalla normativa vigente in materia di protezione dati e dai provvedimenti del garante.

Art. 13 Entrata in vigore

1. Il presente Regolamento entra in vigore il giorno successivo alla pubblicazione all'albo pretorio on-line dell'Ateneo e, parimenti, cessa di avere efficacia il Regolamento per la disciplina dell'utilizzo e la gestione dei sistemi di videosorveglianza presenti nel Polo delle Scienze Sociali che viene abrogato.

2. L'Ateneo dà pubblicità al presente Regolamento tramite la pubblicazione sul sito internet istituzionale nella sezione dedicata ai Regolamenti di Ateneo e nella sezione "Amministrazione Trasparente".

Firenze,

La Rettrice
Prof.ssa Alessandra Petrucci

ALESSANDRA
PETRUCCI
21.10.2022
11:22:59
GMT+01:00

Allegato 1 Modello semplificato informativa

TITOLARE DEL TRATTAMENTO

L' UNIVERSITÀ DEGLI STUDI DI FIRENZE è il Titolare del Trattamento.
Dati di contatto del Responsabile per la Protezione dati:
privacy@adm.unifi.it

FINALITÀ DELLA VIDEOSORVEGLIANZA

Garantire la sicurezza e l'incolumità del personale universitario, degli studenti e dei frequentatori degli spazi universitari. Tutelare il patrimonio dell'Ateneo prevenendo e perseguendo il compimento di eventuali atti illeciti.

PERIODO DI CONSERVAZIONE

I dati raccolti durante l'orario di apertura degli edifici sottoposti a videosorveglianza sono visualizzati in tempo reale tramite i monitor collocati all'interno dei locali di portineria e saranno conservati.
Le immagini eventualmente registrate saranno conservate per un periodo non superiore a 72 ore.
I dati raccolti durante l'orario di chiusura dell'edificio (19.30 - 7.30) sono registrati e conservati per i tempi stabiliti dalla normativa vigente (non superiori a 7 giorni).

DIRITTI DEGLI INTERESSATI

È possibile accedere ai propri dati ed esercitare gli altri diritti riconosciuti dalla normativa in materia di protezione dati rivolgendosi all'indirizzo:
privacy@adm.unifi.it

Ulteriori informazioni sono disponibili all'indirizzo:
www.unifi.it/upload/sub/protezionedati/informativa_videosorveglianza.pdf