UNIVERSITÀ DI FOGGIA
REGOLAMENTO PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA PRESSO LE SEDI DELL'UNIVERSITÀ DEGLI STUDI DI FOGGIA
(emanato con D.R. n. 0000 – 2023, prot. n. 0000 – I/3 del [data])

"I termini relativi a persone che, nel presente Regolamento, compaiono solo al maschile si riferiscono indistintamente a persone di genere femminile e maschile. Si è rinunciato a formulazioni rispettose dell'identità di genere per non compromettere la leggibilità del testo e soddisfare l'esigenza di semplicità dello stesso."

Premessa

1. Il presente Regolamento disciplina il trattamento dei dati personali, effettuato mediante impianti di videosorveglianza collocati presso le sedi dell'Università di Foggia, nel rispetto della vigente disciplina in materia di protezione dei dati personali alla quale si rimanda per ogni ipotesi non prevista dal presente Regolamento, e precisamente:
   a) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (RGPD – GDPR);
   b) D.Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali così come modificato dal D.Lgs. 101/2018 e ss.mm.ii.;
   c) L. 300/1970 Statuto dei Lavoratori;
   d) D.Lgs. 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
   e) Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, Versione 2.0, adottate il 29 gennaio 2020 dal Comitato Europeo per la Protezione dei Dati (CEPD – EDPB).
2. Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di impianti di videosorveglianza nelle sedi universitarie, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Art. 1 - Definizioni

1. Ai fini del presente Regolamento, si richiamano tutte le definizioni contenute nell'art. 4 del GDPR e comunque, si intende per:
   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 del trattamento***", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
d. "**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;
e. "**persone autorizzate**" al trattamento dei dati personali: chiunque agisca sotto l'autorità del titolare del trattamento o sotto quella del responsabile del trattamento, che abbia accesso a dati personali e che venga istruito in tal senso dai medesimi soggetti;
f. "***interessato***": la persona fisica identificata o identificabile;
g. "**GDPR**", il Regolamento Generale sulla Protezione dei Dati, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
h. "***Codice***", il D.Lgs. n. 196/2003, recante Codice in materia di protezione dei dati personali, come modificato dal D.lgs 10 agosto 2018, n. 101;
i. "***Garante***", il Garante per la protezione dei dati personali di cui all'art. 153 del Codice.

Art. 2 – Soggetti

1. Il Titolare del trattamento è l'Università di Foggia, in persona del Magnifico Rettore pro tempore.
2. Il Titolare nomina con atto scritto, per ciascuno o per più impianti di videosorveglianza installati, il Responsabile del trattamento, impartisce direttive per eventuali responsabili trattamento e gli e vigila sull'osservanza delle norme di legge e di Regolamento anche da parte degli stessi responsabili del trattamento ove nominati.
3. Il titolare del trattamento può delegare il Direttore Generale alla visione delle immagini e a compiere ogni opportuna attività sui sistemi di video sorveglianza, incluse la designazione di persone autorizzate con indicazione specifica dei compiti loro assegnati, tra i quali anche la decisione sulla individuazione dei luoghi ove collocare le singole telecamere.
4. Le persone autorizzate o eventuali responsabili del trattamento nominati ex art. 28 del GDPR, previamente formati e istruiti su protezione delle persone fisiche con riguardo al trattamento dei dati personali, devono rispettare il presente Regolamento e la disciplina vigente in materia di protezione dei dati personali, garantendo che:
   a) ciascuna telecamera venga adeguatamente collocata nelle aree individuate e censita con attribuzione di un riferimento univoco, secondo l'autorizzazione mediante decreto del Direttore Generale anche in ordine ad eventuali modifiche della collocazione delle telecamere stesse;
   b) venga individuato l'angolo di visuale e registrazione;
   c) le immagini siano conservate per un periodo massimo di 72 ore, così come previsto dal presente Regolamento;
   d) i dati vengano automaticamente cancellati dopo il già menzionato termine di 72 ore;
   e) vengano eseguite le opportune manutenzioni periodiche degli impianti e che gli stessi siano regolarmente funzionanti.
5. La visione delle immagini registrate (e quindi il trattamento dei dati personali)

è consentita al Magnifico Rettore, al Direttore Generale, ai soggetti addetti alla manutenzione ed alle riparazioni nominati responsabili del trattamento, e – secondo quanto previsto dalla Direttiva (UE) 2016/680 – alle persone autorizzate, alle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.

6. In caso di rilevazioni di immagini di fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza, della tutela ambientale o del patrimonio pubblico, le persone autorizzate provvederanno a darne comunicazione senza ritardo al Magnifico Rettore, al Direttore Generale e al Responsabile della Protezione dei Dati (RPD/DPO), provvedendo, nel contempo, all'acquisizione delle stesse con l'utilizzo della crittografia su idonei supporti informatici al fine di evitare la loro cancellazione mediante sovrascrittura nel periodo di 72 ore come previsto dal presente Regolamento.
7. Tutti gli accessi alle immagini sono documentati mediante l'annotazione in un apposito "registro degli accessi" (cartaceo o informatico), custodito e compilato dalle persone autorizzate, nel quale sono riportati:
   a) data e ora dell'accesso;
   b) i dati del soggetto che esegue l'accesso;
   c) i dati relativi al sistema di video sorveglianza al quale si accede (estremi identificativi della telecamera);
   d) la motivazione all'accesso.

Art. 3 – Finalità

1. Le finalità perseguite attraverso il sistema di video sorveglianza sono conformi a quelle individuate dall'Università di Foggia per tutelare il patrimonio dei beni mobili ed immobili presenti nelle sedi universitarie, prevenire atti vandalici, garantire un adeguato grado di sicurezza alla popolazione universitaria, indagini di polizia giudiziaria, garantire la libertà di svolgimento delle attività didattiche e di ricerca in piena sicurezza. In particolare, si precisano le seguenti finalità, determinate, esplicite e legittime:
   a) prevenzione al fine di garantire la sicurezza e incolumità del personale universitario, degli studenti e dei frequentatori a vario titolo degli spazi universitari;
   b) tutela del patrimonio immobiliare dell'Ateneo;
   c) tutela dei beni mobili dell'Università e degli utenti interni;
   d) prevenzione di eventuali atti vandalici quale ausilio all'accertamento dei fatti da parte delle Autorità di Pubblica Sicurezza;
   e) prevenire e rilevare accessi illeciti e non autorizzati agli spazi di pertinenza dell'Ateneo.
2. La sorveglianza regolare e sistematica e automatizzata di uno spazio specifico con mezzi ottici o audiovisivi comporta la raccolta e la conservazione di informazioni grafiche o audiovisive su tutte le persone che entrano nell'area monitorata, identificabili in base al loro aspetto o ad altri elementi specifici. L'attività di videosorveglianza e di registrazione delle immagini rilevate non è utilizzata per finalità diverse da quelle esplicitate.
3. Gli impianti di video sorveglianza non potranno essere impiegati come strumenti per effettuare controlli sui docenti, sul personale tecnico-amministrativo e sugli studenti, sia con riguardo alle funzioni ed attività da essi svolte all'interno dell'Università, sia con riferimento alle rispettive

abitudini personali.

4. I programmi informatici utilizzati per la video sorveglianza rispettano i principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita ex art. 25 del GDPR con sistemi di crittografia dei dati e sono impostati con la sovrascrittura automatica dopo il termine di 72 ore.

Art. 4 – Raccolta e trattamento dei dati.

1. La raccolta dei dati avviene tramite videocamere installate presso le sedi dell'Università che consentono unicamente riprese video senza riprese audio-foniche. La registrazione delle immagini avviene con videocamere a immagine fissa.

Art. 5 – Conservazione e obbligo di cancellazione dei dati

1. Le immagini registrate dagli impianti di video sorveglianza presso ciascuna delle sedi sono conservate per il tempo necessario al perseguimento delle finalità e, comunque, per un periodo non superiore alle 72 ore dalla loro rilevazione e successivamente automaticamente cancellate con sovra-registrazione e modalità che rendono inutilizzabili i dati cancellati.

Art. 6 - Misure di sicurezza

1. Il titolare del trattamento, ai sensi dell'art. 32 del GDPR, mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, 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.
2. La sicurezza del sistema e dei dati, vale a dire la protezione da interferenze volontarie e involontarie nel suo normale funzionamento, può comprendere:
   a) protezione dell'intera infrastruttura del VSS (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti;
   b) protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione;
   c) cifratura dei dati;
   d) utilizzo di soluzioni basate su hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;
   e) rilevamento di guasti di componenti, software e interconnessioni;
   f) strumenti per ripristinare la disponibilità dei dati personali e l'accesso agli stessi in caso di problemi fisici o tecnici.
3. Il controllo degli accessi garantisce che solo le persone autorizzate possano accedere al sistema e ai dati, mentre agli altri viene impedito di farlo. Le misure che supportano il controllo fisico e logico degli accessi includono:
   a) la garanzia che tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in cui vengono conservate le riprese video siano protetti contro l'accesso non supervisionato da parte di terzi;
   b) il posizionamento dei monitor (soprattutto quando si trovano in zone aperte, come una reception) in modo tale che solo gli operatori autorizzati possano visualizzarli;
   c) la definizione e l'applicazione delle procedure per la concessione, la modifica e la revoca dell'accesso;

d) l'attuazione di metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica;
e) la registrazione e la revisione periodica delle azioni eseguite dagli utenti (con riguardo sia al sistema sia ai dati);
f) l'esecuzione del monitoraggio e l'individuazione di guasti agli accessi in modo continuativo e la risoluzione in tempi brevi delle carenze individuate.

Art. 7 – Obblighi di trasparenza e informazione

1. Le informazioni di primo livello (segnale di avvertimento/cartello) riguardano la modalità con cui avviene la prima interazione fra il titolare del trattamento e l'interessato.
2. Le informazioni di primo livello (segnale di avvertimento) devono comunicare i dati più importanti, quali le finalità del trattamento, l'identità del titolare del trattamento, l'esistenza dei diritti dell'interessato, i legittimi interessi perseguiti dal titolare, i recapiti del responsabile della protezione dei dati, l'eventuale trasmissione di dati a terzi in particolare se ubicati al di fuori dall'UE, e il periodo di conservazione.
3. 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.
4. Le informazioni di secondo livello devono essere facilmente accessibili per l'interessato, mediante informativa completa contenuta in un pagina web oppure su cartelloni posizionati o affissi in un luogo di facile accesso. È preferibile che nelle informazioni di primo livello si faccia riferimento a una fonte digitale (ad esempio, un codice QR o un indirizzo web) per le informazioni di secondo livello. In ogni caso, le informazioni devono essere facilmente disponibili anche in formato non digitale. Dovrebbe essere possibile accedere al secondo livello di informazioni senza entrare nell'area videosorvegliata, soprattutto se le informazioni sono fornite digitalmente (ad esempio, tramite un link). In ogni caso, le informazioni devono contenere tutti gli elementi obbligatori a norma dell'articolo 13 del GDPR.
5. In prossimità delle aree in cui è installata ciascuna telecamera e comunque prima di entrare nella zona sorvegliata è affisso un segnale di avvertimento contenente le informazioni come indicato nei commi precedenti.
6. Il segnale di avvertimento con l'informativa è realizzato secondo lo schema riportato nelle linee guida 3/2019 del Comitato Europeo per la Protezione dei Dati.

Art. 8 – Comunicazione dei dati

1. La comunicazione a soggetti pubblici dei dati personali acquisiti mediante i sistemi di videosorveglianza è ammessa solo se prevista da norma di legge o di regolamento oppure, in mancanza, quando è necessaria per lo svolgimento delle funzioni istituzionali, previa comunicazione al Garante.
2. Oltre a quanto previsto dall'articolo 3, comma 4, del presente Regolamento, le

immagini rilevate dagli impianti di video sorveglianza potranno essere comunicate anche ai soggetti pubblici ai sensi dell'art. 58, comma 2, del Codice privacy per fini di sicurezza nazionale o difesa.

3. La comunicazione e la diffusione devono essere in ogni caso autorizzate dal Titolare del trattamento ai sensi dell'art. 3 del presente Regolamento.

Art. 9 - Diritti dell'interessato

1. Gli interessati possono esercitare i diritti previsti dagli articoli dal 15 al 22 del Regolamento UE 2016/679, e precisamente:
   a) chiedere la conferma dell'esistenza o meno di propri dati personali (art. 15).
   b) accedere in ogni momento ai dati che la riguardano (art. 15).
   c) ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione (art. 15).
   d) ottenere la rettifica l'aggiornamento, l'integrazione, (art. 16) o, nel caso i dati siano trattati in violazione di legge oppure incompleti o errati, la cancellazione dei dati o il blocco (art. 17).
   e) ottenere la limitazione del trattamento (art. 18).
   f) ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad un altro titolare del trattamento senza impedimenti (art. 20).
   g) opporsi al trattamento dei propri dati in qualsiasi momento per motivi legittimi (art. 21).
   h) opporsi ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (art. 22).
2. La richiesta dovrà essere indirizzata a (indicare indirizzo e-mail dove poter inviare richieste es.: privacy@unifg.it – NO quello del DPO).

Art. 10 - Informativa agli interessati

1. L'Università di Foggia informa gli interessati in ordine alla presenza negli spazi universitari di sistemi di video sorveglianza mediante l'affissione, nelle zone interessate e in prossimità della videocamera, della segnaletica di avvertimento (All. n. 1) realizzata secondo lo schema riportato nelle linee guida 3/2019 del Comitato Europeo per la Protezione dei Dati che indichi, nel contenuto, sia le necessarie informazioni di primo livello, sia quelle di secondo livello così come descritte nelle menzionate linee guida.

Art. 11 - Entrata in vigore e pubblicità.

1. Il presente Regolamento entra in vigore alla data del relativo decreto di emanazione.

Versione 2023-01