IL RETTORE

Visto lo Statuto dell'Università degli Studi di Palermo;

Vista la delibera del Consiglio di Amministrazione dell'Università degli Studi di Palermo n. 08/27 del 16/09/2024 (repertorio n. 1164 prot. n. 147093/2024);

DECRETA

di emanare il

REGOLAMENTO PER LA GESTIONE DEI DATI TRAMITE IL SISTEMA DI VIDEOSORVEGLIANZA

Art. 1 - OGGETTO

1. L'Università degli Studi di Palermo (di seguito anche "Università" o "Ateneo"), in considerazione delle caratteristiche delle proprie sedi, dell'estensione del territorio del *Campus* Universitario (Parco d'Orléans-Viale delle Scienze), dell'articolazione delle sue strutture e delle sue infrastrutture, ritiene indispensabile l'impiego di un sistema di videosorveglianza intelligente, nelle aree dedicate alle attività istituzionali, a tutela delle persone e del patrimonio mobile e immobile di cui dispone, nel rispetto dei principi di necessità e proporzionalità.
2. Il sistema è realizzato per mezzo di una piattaforma, integrata ed innovativa, di video analisi, videosorveglianza e controllo degli accessi, che prevede telecamere sia nuove sia preesistenti di terze parti.
3. Il presente Regolamento disciplina l'utilizzo e il funzionamento del sistema di videosorveglianza intelligente installato nelle zone interne ed esterne di pertinenza delle strutture e sedi delle quali l'Università degli Studi di Palermo è titolare del trattamento dei dati personali acquisiti attraverso l'uso di tali sistemi, in conformità alle disposizioni del vigente Regolamento UE 27 aprile 2016, n. 679 (GDPR), del Decreto Legislativo 30 giugno 2003, n. 196 (Codice privacy) e ss.mm.ii, Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), delle Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate dal Comitato europeo per la protezione dei dati il 29 gennaio 2020, del vigente Regolamento di Ateneo in materia di protezione dei dati personali, nonché agli inerenti provvedimenti ed atti interpretativi e di indirizzo.
4. L'Università utilizza i sistemi di videosorveglianza, nell'ambito delle proprie finalità istituzionali, in considerazione delle sue specifiche caratteristiche organizzative, della distribuzione delle sue sedi e le particolarità strutturali degli edifici e dei locali, al fine di rafforzare la sicurezza e l'incolumità del personale, degli studenti e di chi frequenta l'ambiente universitario a vario titolo, di proteggere e tutelare il patrimonio mobiliare e immobiliare e le risorse dell'Ateneo.
5. Il trattamento dei dati personali, effettuato mediante impianti di videosorveglianza negli ambienti dell'Università, si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, garantendo altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.
6. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nel presente regolamento e non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria e quanto previsto dalle vigenti norme e dal presente regolamento.

Art. 2 – RIFERIMENTI NORMATIVI

1. Nel definire il contenuto del presente regolamento si sono considerati:
   - il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, di seguito denominato "GDPR";
   - il Decreto Legislativo 196/2003 recante "Codice in materia di protezione dei dati personali" e successive modifiche e integrazioni, di seguito denominato "Codice";
   - il Decreto Legislativo 101/2018 (Decreto di armonizzazione della normativa nazionale al Regolamento UE 2016/679);
   - la Legge 7 agosto 1990, n. 241, recante "Norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", come successivamente modificata;
   - l'art. 391 quater del Codice di procedura penale, di seguito denominato "CPP";
   - il provvedimento generale dell'Autorità garante per la protezione dei dati personali in materia di videosorveglianza dell'8 aprile 2010;
   - le Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video del Comitato europeo per la protezione dei dati;
   - Legge n. 300/1970, recante lo Statuto dei Lavoratori, con particolare riferimento all'art. 4;
   - Regolamento (UE) 2024/1689 del 13.06.2024 sull'intelligenza artificiale;
   - Vigente Regolamento dell'Università in materia di protezione dei dati personali;

Art. 3 - DEFINIZIONI

1. Ai fini del presente regolamento, per le definizioni si fa espresso riferimento a quanto previsto dall'art. 4 del GDPR, in particolare:
   a) dato personale: qualsiasi informazione relativa a persona fisica, identificata o identificabile ("interessato"), anche indirettamente, mediante riferimento ad un indicativo come: il nome, un numero di identificazione, dati sull'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 anche senza l'ausilio di processi automatizzati, e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione e la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati;
   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) autorizzato al trattamento: il personale che, limitatamente allo svolgimento delle attività istituzionali di rispettiva competenza connesse con le attribuzioni dell'incarico ricoperto, compie operazioni di trattamento sotto l'autorità del titolare o del responsabile del trattamento;
   f) interessato: la persona fisica, cui si riferiscono i dati personali;
   g) violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

h) blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento, compresa la cancellazione.

Art. 4 - AMBITO DI APPLICAZIONE

1. Il presente regolamento si applica al sistema di videosorveglianza intelligente installato presso i locali e le aree di pertinenza dell'Università di Palermo che comporta un trattamento di dati personali.
2. Tale sistema inquadra aree esterne e interne di pertinenza dell'Ateneo, in cui transitano vari soggetti (dipendenti dell'Ateneo, fornitori, visitatori, studenti).
3. Sono chiamati ad applicare e rispettare il presente regolamento il Titolare, i Responsabili Interni in materia di protezione dei dati personali dell'Università unitamente ai Referenti e Autorizzati al trattamento da questi designati, l'Area Sistemi Informativi e le altre Aree per gli ambiti di competenza, gli eventuali Responsabili esterni del trattamento.

Art. 5 - PRINCIPI

1. Il trattamento legato all'impiego di videosorveglianza si fonda sui principi applicabili al trattamento di dati personali di cui all'art. 5 del GDPR. Sulla base di tali principi i dati personali devono essere:
   a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principio di liceità, correttezza e trasparenza);
   b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (principio di limitazione della finalità);
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione dei dati);
   d) esatti e, se necessario, aggiornati (principio di esattezza);
   e) conservati in una forma che consenta l'identificazione degli interessati, nei limiti consentiti dalle vigenti norme, per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di limitazione della conservazione);
   f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di integrità e riservatezza);
   g) nella progettazione e attivazione vengono assunte tutte le misure tecniche e organizzative necessarie per evitare la raccolta di dati di particolari categorie di cui all'art. 9 del GDPR;
   h) gli apparati di ripresa digitali connessi a reti informatiche devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615 ter del Codice penale. La trasmissione di immagini riprese da apparati di videosorveglianza tramite una rete pubblica deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless;
   i) è escluso: l'acquisto e l'uso delle funzioni di riconoscimento facciale/categorizzazione biometrica e riconoscimento targhe; l'utilizzo di lettori biometrici.

2. L'installazione e l'utilizzo del sistema di videosorveglianza intelligente deve essere effettuato tenendo conto dei suddetti principi.

Art. 6 - FINALITA' E BASI GIURIDICHE

1. Le finalità perseguite mediante l'attivazione del sistema di videosorveglianza intelligente indicato all'art. 4 del presente regolamento sono le seguenti:
   a) sicurezza e incolumità del personale universitario, degli studenti e dei frequentatori a vario titolo degli spazi universitari;
   b) prevenzione e tutela nei confronti di reati contro il patrimonio mobiliare e immobiliare dell'Università di Palermo;
   c) protezione della proprietà e delle risorse universitarie;
   d) accertamento e prova di eventuali incidenti e sinistri avvenuti sulle aree interne;
   e) accertamento e prova di comportamenti illeciti, attuabili ex post in ragione di concreti indizi, (c.d. controlli difensivi, in "senso stretto", a tutela del patrimonio e dell'immagine dell'ente) purché diversi dal mero inadempimento della prestazione lavorativa e, comunque, nel rispetto dei presupposti di legittimità di cui all'art. 4 dello Statuto dei Lavoratori.
2. L'utilizzo del sistema citati comporta un trattamento di dati personali, da effettuare nel rispetto degli obblighi stabiliti dalla normativa in materia di protezione dei dati personali.
3. Il trattamento si fonda sulle seguenti basi giuridiche:
   a) il trattamento 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 ovvero in adempimento a obblighi di legge o di regolamento (cfr. art. 6, par. 1, lett. c) ed e), e par. 3 lett. b), del GDPR, nonché art. 2-ter del Codice privacy).
      Si precisa che, ai sensi dell'art. 2-ter comma 1 del Codice privacy, la base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del Regolamento è costituita da una norma di legge o di regolamento o da atti amministrativi generali.
   b) L'attività di videosorveglianza è basata sul perseguimento del legittimo interesse (articolo 6, paragrafo 1, lettera f), del GDPR) dell'Ateneo o di un terzo, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.
      i) Nel caso di specifiche richieste delle Forze dell'ordine e dell'Autorità giudiziaria, la base giuridica è costituita dall'obbligo di legge.
      ii) Per quanto riguarda la ripresa di aree in cui sono presenti i lavoratori dell'Ateneo, si provvede a sottoporre apposito accordo sindacale alle rappresentanze, ai sensi dell'art 4 dello Statuto dei lavoratori, ovvero, in mancanza di accordo si chiede l'autorizzazione alla sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, qualora siano interessate sedi dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro.

Art. 7 - INFORMATIVE

1. Agli interessati va fornita apposita informativa privacy (art. 13 del GDPR) che deve essere consultabile anche in inglese (e se possibile pure in altre lingue), in considerazione che l'Ateneo è frequentato anche da utenti stranieri (studenti, dottorandi, docenti, ricercatori, convegnisti, ecc.), per facilitarne la consultazione.
2. L'informativa viene gestita su un doppio livello.
3. Il primo livello è gestito attraverso un modello semplificato di informativa "minima" (fornito dal Comitato europeo per la protezione dei dati nelle Linee guida 3/2019), contenente le informazioni essenziali sul trattamento (titolare, dati di contatto dell'eventuale RPD, finalità, conservazione e modalità di esercizio dei diritti).
4. Tali informazioni devono essere fornite prima che abbia inizio il trattamento (quindi prima che l'interessato entri nell'area videosorvegliata) e devono essere gestite in modo che siano facilmente accessibili. A tal fine, considerando quanto già indicato dal Garante privacy nel suo provvedimento del 2010 e quanto riportato nelle Linee guida 3/2019 del Comitato europeo per la protezione dei dati, nel posizionare il cartello sulla videosorveglianza occorre tener conto delle seguenti indicazioni:

a) il cartello deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
b) il cartello deve essere posizionato approssimativamente a livello degli occhi;
c) il formato e il posizionamento del cartello deve essere tale da renderlo chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
d) non è necessario specificare l'esatta posizione delle telecamere, purché non vi siano dubbi su quali aree siano soggette a monitoraggio e il contesto della sorveglianza sia chiarito in modo inequivocabile;
e) l'interessato deve essere in grado di valutare l'area ripresa in modo da poter evitare di essere inquadrato o da adattare il suo comportamento, se necessario;
f) in presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.

5. L'interessato deve poter accedere alle ulteriori informazioni previste dall'art. 13 del GDPR. A tal fine va gestita l'informativa completa (secondo livello), inserendo nel cartello le modalità con cui l'interessato può prenderne visione.
6. Nel definire le modalità con cui rendere accessibile l'informativa di secondo livello occorre ricordare di individuare sempre, accanto a modalità digitali, anche una modalità tradizionale, come un numero telefonico da contattare.

Art. 8 - RUOLI PRIVACY

1. Il Titolare del trattamento dei dati è l'Università degli studi di Palermo, alla quale compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.
2. Il Titolare può ricorrere a soggetti esterni, che presentino garanzie sufficienti, per mettere in atto misure tecniche e organizzative adeguate a garantire il rispetto delle disposizioni normative in materia di protezione dei dati personali e dei diritti degli interessati.
3. Le persone che operano sotto l'autorità dell'Ateneo devono ricevere apposita nomina, completa delle istruzioni da seguire nello svolgimento delle attività di competenza.
4. L'individuazione è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun autorizzato tenendo conto dei diversi ruoli e mansioni.
5. Gli autorizzati devono essere istruiti sul corretto uso del sistema, sulle disposizioni della normativa di riferimento e sul presente Regolamento e devono conformare la propria condotta al pieno rispetto del medesimo.
6. I soggetti esterni che svolgono attività per conto dell'Ateneo quali responsabili del trattamento devono sottoscrivere apposito accordo contenente le specifiche previste dall'art. 28 del GDPR.

Art. 9 - CARATTERISTICHE DEL SISTEMA

1. L'individuazione dei sistemi di videosorveglianza dell'Università è descritta in appositi documenti custoditi dall'Area Sistemi Informativi di Ateneo. In tali documenti vengono altresì specificati i presupposti per la legittimità della progettazione e dell'acquisto di ciascun impianto di videosorveglianza e/o gruppo di telecamere, le relative caratteristiche tecniche e le misure tecniche e organizzative previste in ossequio ai principi di liceità, necessità, proporzionalità del GDPR.
2. Fermi restando gli obblighi dei responsabili di struttura individuati dal regolamento in materia di protezione dei dati personali dell'Università quali responsabili interni, il Dirigente dell'Area Sistemi Informativi è individuato quale soggetto designato ai sensi dell'art. 2 quaterdecies del D.lgs. n. 196/2003 (Codice Privacy) ai fini dell'applicazione del presente regolamento.

3. Si riportano di seguito le principali caratteristiche dell'attuale sistema che, in caso variazioni, verranno aggiornate fermo restando che, in ogni caso, fanno fede i documenti di cui al comma 1 del presente articolo:
   a. Il sistema è operativo 24 ore su 24, 7 giorni su 7.
   b. Il sistema consente sia la visione *real time* delle immagini che la loro registrazione con visione successiva.
   c. Il sistema può rilanciare la visione anche su dispositivi specifici che hanno le pattuglie della società di vigilanza (client aziendale ad accesso con operatore).
   d. I dispositivi che consentono la visione da remoto ricevono i flussi definiti per l'utente dopo la sua autenticazione e la stabilizzazione del tunnel ipsec VPN per dialogare con i server.
   e. La visione *real time* delle immagini avviene tramite applicativo ACC Client su singola vista o viste multiple preimpostate; ogni client può pilotare 4 monitor ed è possibile sezionare il monitor con più inquadrature;
   f. La registrazione delle immagini viene effettuata su sistema di registrazione composto da Network Video Recorder (NVR), posti nel Data Center dell'Ateneo, che si occupano del management e delle registrazioni per tutte le telecamere di sistema. In termini funzionali, le immagini live riprese dalle telecamere IP verranno trasmesse tramite la LAN di accesso e trasporto verso gli NVR, che si occuperanno di registrare senza soluzione di continuità gli stream video ricevuti da ciascuna telecamera, conservandoli sui propri HDD interni.
   g. La visione live delle riprese ed il playback delle registrazioni saranno possibili attraverso la Graphical User Interface (GUI) dell'applicativo client, in esecuzione sulle workstation degli operatori.
   h. Il tempo di conservazione è fissato a 48 ore. Rimangono salve speciali esigenze di ulteriore conservazione connesse a festività o periodi di chiusura delle sedi dell'Università, da definire all'occorrenza con appositi e motivati Decreti Rettorali, ovvero a specifiche richieste di autorità giudiziaria o polizia giudiziaria, per finalità di prevenzione, accertamento o repressione di reati.
   i. La cancellazione delle immagini avviene tramite un sistema di sovrascrittura.
   j. Non vengono effettuate rilevazioni audio: nel sistema i soli apparati che permettono di rilevare anche l'audio sono i Point of Presence e i multi-sensori ambientali. I primi sono apparati citofonici che vengono attivati dal soggetto solo quando viene premuto un pulsante di sos che permette di mettere in comunicazione audio-video il soggetto con la centrale operativa; il secondo permette di attivare un allarme presso la centrale operativa solo su un livello prestabilito di decibel, tipo sparo, esplosione o forti grida.
   k. Il sistema non consente la rilevazione di dati particolari.
   l. Non sono state acquistate le licenze e non sono attivate le funzioni di riconoscimento facciale e targhe.
   m. Non vengono effettuati trattamenti di dati biometrici.
   n. Sono attivate funzioni di intelligenza artificiale. Il Sistema utilizza due tipologie di modelli di AI.
      . Il primo modello è on-board su tutte le telecamere oggetto della fornitura ed è finalizzato alla classificazione degli oggetti inquadrati in una scena e al rilevamento automatico delle variazioni degli oggetti da una base-line definita nel tempo in autoapprendimento. Il secondo modello è implementato nei server NVR ed è finalizzato ad implementare funzionalità avanzate di ricerca.
      . Il secondo modello è utilizzato direttamente nei server NVR e rielabora il flusso video di telecamere senza AI on-board in modo da rendere tali telecamere con le stesse funzionalità di quelle oggetto della fornitura.
   o. Le immagini acquisite vengono utilizzate per addestrare l'algoritmo di intelligenza artificiale sia on-board che sulle NVR e il tutto è finalizzato a migliorare le funzionalità

impiegate dal sistema. Nessun parametro è inviato al fornitore del sistema ai fini di migliorare l'algoritmo.

4. Tutti i modelli AI presenti nel Sistema hanno la finalità di definire scenari di anomalia e far scattare un allarme sul pannello del "centro di Attenzione" che permette all'operatore della Control room di prendere il Focus in tempo reale delle camere soggette ad anomalia.
5. L'appliance AI presente nel sistema permette la ricerca delle scene d'interesse attraverso l'ausilio dell'Artificial Intelligence (AI), per semplificare l'attività da parte dell'operatore nell'individuare un soggetto (persona o veicolo) tra tutte le telecamere Avigilon che compongono il sistema.
6. L'analisi video di Avigilon è di tipo ad autoapprendimento, ovvero la telecamera si adatta ed "impara" la scena, vedendo il semplice movimento delle persone al suo interno. Nessun parametro è inviato al fornitore del sistema ai fini di migliorare l'algoritmo.
7. Gli efficienti strumenti di ricerca consentono di cercare velocemente, all'interno di un video registrato, i movimenti, la presenza di oggetti classificati (persone o veicoli), le variazioni della scena sullo sfondo (ricerca di miniature) e gli eventi.
8. Attraverso l'immediata indicizzazione di tutti i Dati/Immagini contenuti nel data base e grazie ad un potente motore di ricerca è possibile effettuare ricerche di Immagini/Eventi in tempo reale, con diverse modalità di analisi.
9. Il sistema fornisce allarmi automatici per anomalie sulla ripresa, sui dati del sensore ambientale e sugli eventuali sos degli intercom POP, solo alla sala operativa.
10. Il sistema viene compiutamente descritto nella relazione tecnica che si allega.

Art. 10 - VALUTAZIONE DI IMPATTO

1. In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), GDPR e alle indicazioni contenute nelle Linee guida del gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248 del 2017), è stata effettuata la valutazione di impatto per il trattamento svolto tramite il sistema di videosorveglianza intelligente installato.

Art. 11 - MODALITÀ DI RACCOLTA E TRATTAMENTO DEI DATI

1. La raccolta dei dati avviene tramite le telecamere che compongono il sistema.
2. Le telecamere sono posizionate come da planimetrie, allegate alla relazione tecnica, suscettibili di aggiornamenti che dovranno essere approvati dal Consiglio di Amministrazione.
3. Il raggio di azione delle telecamere installate è impostato in modo tale da inquadrare solo le aree, interne ed esterne, di interesse per le finalità perseguite.
4. Sono escluse dalle riprese aree private (come giardini, ingressi o interni di abitazioni private o di attività commerciali e aziendali …) e aree dedicate ai dipendenti (come aree relax o spogliatoi).
5. Non si effettuano riprese audiofoniche distinguibili.
6. Tutte le inquadrature delle aree interne alle strutture dell'Ateneo sono finalizzate a riprendere i punti di accesso, i corridoi e gli accessi alle aule. Non sono previste inquadrature sulle postazioni di lavoro del personale, né sui rilevatori di presenza, né nelle aree di ristoro. Non è possibile escludere le riprese su distributori di bevande o snack in quanto utilizzati anche dagli studenti e dai visitatori e installati, per comodità logistica, in prossimità delle zone di ingresso. In tal caso, laddove non sia comunque possibile direzionare le videocamere in modo da riprendere solo i dati necessari al controllo degli ingressi, vengono adottate misure tecniche atte ad escludere le riprese, durante le ore di svolgimento di attività, su tali aree di ristoro poste all'interno delle strutture.
7. All'interno delle strutture dove si trovano uffici e/o si svolgono attività di didattica, studio e ricerca (aule didattiche e di studio, biblioteche, laboratori, spazi dedicati agli studenti

o alle loro associazioni), laddove dovesse valutarsi assolutamente indispensabile l'utilizzo della videosorveglianza per tutelare l'immobile e i beni mobili, le riprese sono circoscritte alle sole aree interessate e le telecamere vengono attivate solo negli orari di chiusura delle strutture. In ogni caso, le telecamere non vengono attivate in occasione di eventuali attività extradidattiche o extralavorative che si svolgono all'interno della struttura.

8. Non devono essere installate apparecchiature specificamente 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 devono essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza, il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa o dell'attività diversa espletata.
9. La ripresa di aree esterne in cui sono presenti i lavoratori è limitata alle aree dove gli stessi possono transitare o trovarsi saltuariamente.
10. Le immagini sono registrate su sistema di registrazione composto da Network Video Recorder (NVR), posti nel Data Center dell'Ateneo, con accesso controllato.
11. Il sistema raccoglie solo dati strettamente necessari per il raggiungimento delle finalità perseguite, rilevando e/o registrando solo le immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando (quando non strettamente indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.
12. È fissato un termine decorso il quale le immagini vengono cancellate mediante sovrascrittura. Restano salve speciali esigenze di conservazione in relazione a festività o chiusura delle sedi universitarie, nonché in caso di specifica richiesta dell'Autorità giudiziaria o di Polizia giudiziaria, per finalità di prevenzione, accertamento o repressione di reati, e/o comunque sorgano esigenze difensive.
13. Il sistema di videoregistrazione impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
14. In caso di cessazione del trattamento, i dati personali sono distrutti.
15. La visione delle immagini real-time e l'accesso alle immagini registrate è consentita al solo personale autorizzato per dare seguito a specifiche richieste previste dalla normativa di settore applicabile.
16. Per ogni accesso al sistema di videosorveglianza verrà registrato automaticamente dal sistema il codice dell'utenza che lo ha effettuato (log) che sarà conservato per almeno 6 mesi.
17. L'estrapolazione dei dati è ammessa solo quando sia stata richiesta la copia dei dati nelle ipotesi disciplinate dai punti 13 e 14 del presente regolamento, nel rispetto della normativa di settore applicabile, può essere effettuata solo in presenza contemporanea di due operatori sul sistema.
18. In ordine alle richieste di copia nel caso di fatti di reato, si chiarisce che, essendo consentito solo all'Autorità Giudiziaria e alla Polizia Giudiziaria acquisire copia delle immagini, non è possibile fornire direttamente ai cittadini copia delle stesse ed essi non possono presentare direttamente richiesta di estrapolazione. In presenza di un fatto reato, il cittadino può, entro il termine di conservazione, richiedere il blocco delle immagini ai sensi del punto 13 del presente regolamento, ed esse saranno conservate sospendendo ogni ulteriore trattamento in attesa che la forza di Polizia presso cui verrà proposta denuncia querela faccia apposita richiesta.
19. In caso di intervento di altra forza dell'Ordine, è opportuno seguire la medesima procedura prevista per i fatti reato.
20. Ai sensi dell'art. 391 quater del C.P.P., gli avvocati hanno titolo ad avere copia delle immagini registrate, pertanto esse potranno essere estrapolate, purché la richiesta venga presentata in qualità di difensori d'ufficio/di fiducia di un indagato in procedimento penale. Anche in questo caso la richiesta (motivata) deve essere presentata entro il

termine conservazione e sarà possibile provvedere alle spese per il rilascio di copia di singolo filmato, riversato su apposito supporto.

Art. 12 - SICUREZZA DEI DATI

1. I dati raccolti mediante i sistemi indicati dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio.
2. Ai sensi dell'art. 32, comma 2, del GDPR, nel valutare l'adeguato livello di sicurezza, il Titolare tiene conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'Ateneo.
3. Nella valutazione di impatto sono stati descritti i rischi e le misure adottate.
4. Nel caso di eventuali violazioni di sicurezza, occorre verificare se la violazione comporti dei rischi per gli interessati e procedere, nel caso, alla notifica al Garante privacy e, se si tratta di rischi elevati, alla comunicazione agli interessati.

Art. 13 - ACCESSO AI DATI

1. L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità di cui al punto 6 del presente Regolamento.
2. L'accesso alle immagini è consentito esclusivamente:
   a) al Titolare, al Responsabile e agli autorizzati del trattamento;
   b) alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero);
   c) alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo;
   d) alla società di vigilanza;
   e) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 14. L'accesso da parte dell'interessato sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, verrà pertanto utilizzata una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;
   f) ai soggetti legittimati all'accesso ai sensi e per gli effetti della L. 241/90. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante;
   g) ai difensori di fiducia o d'ufficio di persona indagata che facciano richiesta di avere copia delle immagini, ai sensi dell'art. 391 quater c.p.p.

3. Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito "registro degli accessi" (cartaceo o informatico), nel quale sono riportati:
   a) la data e l'ora dell'accesso;
   b) l'identificazione del terzo autorizzato;
   c) i dati per i quali si è svolto l'accesso;
   d) gli estremi e la motivazione dell'autorizzazione all'accesso;
   e) le eventuali osservazioni dell'incaricato;
   f) la sottoscrizione del medesimo.

4. Per facilitare le richieste di blocco delle immagini in attesa degli accertamenti da parte delle Forze di Polizia o dell'Autorità giudiziaria e di istanze presentate dal difensore, ai sensi dell'art. 391 quater c.p.p., possono essere utilizzate le apposite schede di richiesta blocco e accesso immagini redatte dall'Ateneo.

Art. 14 - DIRITTI DELL'INTERESSATO

1. In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss. del GDPR, su presentazione di apposita istanza, ha diritto:
   a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
   b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
   c) di richiedere la cancellazione qualora sussista uno dei motivi stabiliti dalle richiamate disposizioni, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano;
   e) di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. L'istanza per l'esercizio dei diritti dell'interessato è presentata secondo le indicazioni riportate nell'informativa privacy e nella procedura sulla gestione dei diritti adottata dall'Ateneo.

Art. 15 - MEZZI DI RICORSO, TUTELA AMMINISTRATIVA E GIURISDIZIONALE

1. Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante privacy, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss del GDPR e a quanto disposto dal Codice privacy e s.m.i.

Art. 16 - DIRITTO AL RISARCIMENTO, RESPONSABILITA' E DANNI CAGIONATI PER EFFETTO DEL TRATTAMENTO DEI DATI

1. Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi delle disposizioni di cui all'art. 82 del GDPR.
2. Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
3. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2, GDPR.

Art. 17 - NORME DI RINVIO

1. Per tutto quanto non disciplinato dal presente Regolamento si fa rinvio al Regolamento UE 2016/679 (GDPR), D.lgs. n. 196/2003 e ss.mm.ii., Provvedimento in materia di videosorveglianza 8 aprile 2010 (nonché alla normativa ivi richiamata) dell'autorità Garante per la protezione dei dati personali, alle Leggi vigenti, ai provvedimenti attuativi delle medesime, alle decisioni del Garante privacy, alla Legge 300/1970 e ss.mm.ii., al

Regolamento (UE) 2024/1689 del 13.06.2024 sull'intelligenza artificiale, al vigente Regolamento dell'Università in materia di protezione dei dati personali e ad ogni altra normativa, speciale, generale, nazionale e comunitaria in materia di protezione e trattamento dei dati personali nell'ambito della videosorveglianza.

Art. 18 - ENTRATA IN VIGORE E PUBBLICITÀ

1. Il Presente Regolamento entra in vigore dal giorno successivo alla data di pubblicazione, nell'Albo d'Ateneo, del relativo Decreto Rettorale di emanazione.

Il Rettore
Prof. Massimo Midiri

Firmato digitalmente da: Massimo Midiri
Organizzazione: UNIVERSITA' DEGLI STUDI DI PALERMO/80023730825
Data: 04/11/2024 15:23:43