REGOLAMENTO IN MATERIA DI VIDEOSORVEGLIANZA

Emanato con DR. Rep. n. 485/2019, prot. n. 127287/I/003, del 25.7.2019

Premessa

L'Università degli Studi di Bergamo, per le proprie peculiarità organizzative, la dislocazione territoriale e le caratteristiche strutturali degli edifici, nell'intento di voler garantire una maggiore attenzione alla tutela delle persone (studenti, docenti, personale amministrativo) e alla sicurezza interna ed esterna agli edifici nonché degli impianti, intende dotarsi, nel rispetto dei principi di necessità e proporzionalità, di sistemi di videosorveglianza nei diversi spazi in cui si svolgono le attività istituzionali.
Si precisa che le immagini riguardanti le persone, qualora rendano possibile l'identificazione del soggetto al quale si riferiscono, costituiscono dati personali. La videosorveglianza dà luogo, pertanto, a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.
Il presente Regolamento disciplina il funzionamento dei sistemi di videosorveglianza installati in prossimità degli accessi e all'interno delle strutture dell'Università degli Studi di Bergamo (d'ora in poi Università) e garantisce che il trattamento dei dati personali registrati dai sistemi di videocamera si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.
Per quanto non espressamente previsto dal presente Regolamento, si rinvia integralmente alle norme in materia di tutela dei dati personali (Regolamento UE Generale sulla Protezione dei Dati 2016/679 - RGDP; D. Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 101/2018; Garante per la protezione dei dati personali - Provvedimento in materia di videosorveglianza 8 aprile 2010), nonché alla L. 300/1970.

Articolo 1 – Definizioni

1. Ai fini del presente Regolamento, si intende:
- per «*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;
- 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;
- per «*banca dati*», il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;
- per «*profilazione*», qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- per «*pseudonimizzazione*», il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- per «*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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- per «*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;
- per «incaricato del trattamento», la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del responsabile del trattamento;
- per «*interessato*», la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
- per «*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;
- per «*violazione dei dati personali*», la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- per «*comunicazione*», il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per «*diffusione*», il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per «*dato anonimo*», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Articolo 2 - Principi generali

1. La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configurano un trattamento di dati personali.

2. Il trattamento di dati personali attraverso sistemi di videosorveglianza da parte dell'Università avviene esclusivamente nell'ambito dello svolgimento delle funzioni istituzionali.

3. La determinazione della dislocazione delle videocamere e delle modalità di ripresa e il trattamento dei dati raccolti vengono effettuati in osservanza dei seguenti principi:

- *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 in ossequio al disposto di cui all'art. 6, Paragrafo 1, lett. e), RGPD.
- *Principio di necessità*: in applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.

- *Principio di proporzionalità*: la raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.
Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere.

- *Principio di finalità*: ai sensi dell'art. 5, Paragrafo 1, lett. b), RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità.
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, l'Università procederà all'effettuazione della Valutazione d'impatto sulla protezione dei dati, in conformità a quanto previsto all'art. 35 RGPD.

Articolo 3 – Finalità

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

2. Si provvede alla raccolta di 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.

Articolo 4 – Soggetti (Titolare, Designato, Responsabili del Trattamento dei dati e Incaricati)

1.Il Titolare dei trattamenti di dati personali effettuati mediante sistemi di videosorveglianza installati presso l'Università e l'Università stessa, intesa come persona giuridica, rappresentata dal suo Legale Rappresentante, il Magnifico Rettore pro tempore. All'Università 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 Responsabile del Servizio di Prevenzione e Protezione (RSPP) è individuato quale soggetto Designato a gestire il trattamento dei dati personali rilevati attraverso il sistema di videosorveglianza.
Il Designato ha l'obbligo di attenersi a quanto previsto dalla normativa vigente in tema di trattamento dei dati personali, ivi incluso il profilo della sicurezza, ed alle disposizioni del presente Regolamento.
Il Designato procede al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni previste dalla normativa vigente sulla privacy e delle proprie istruzioni.
Le competenze proprie del Designato sono analiticamente disciplinate nell'atto giuridico avente forma scritta, con il quale il Titolare provvede alla sua individuazione.

3. Il Titolare e il Designato possono ricorrere a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato, in tutti i casi in cui egli, per la gestione/assistenza 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, il Designato 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.

4. L'individuazione degli Incaricati è effettuata per iscritto e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun Incaricato, specificando se il trattamento consiste nella sola visione delle immagini registrate e/o nell'accesso alle immagini registrate ed alla possibilità di estrazione delle stesse.
In ogni caso, prima dell'utilizzo degli impianti, gli Incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.
Gli Incaricati procedono al trattamento attenendosi alle istruzioni impartite dal Designato il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.
In particolare, gli Incaricati devono:

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle proprie mansioni o funzioni istituzionali;
- custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare banche dati nuove senza autorizzazione espressa del Titolare del trattamento;
- conservare e trattare i dati rispettando le misure di sicurezza predisposte dall'Università;
- fornire al Designato, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Articolo 5 - Raccolta e trattamento dei dati

1. La raccolta dei dati avviene tramite videocamere aventi le caratteristiche tecniche descritte in un apposito documento conservato agli atti della Direzione Generale. In ragione di sopraggiunte nuove implementazioni per effetto di novità tecnologiche e/o esigenze per rispondere alle finalità di cui al precedente articolo 3, il Titolare del trattamento dei dati provvederà a modificare il documento nel rispetto di quanto previsto dal presente Regolamento e previa informazione alle OO.SS., alle RSU e agli Organi competenti.

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 saranno orientate sui lettori badge né, all'interno né sulle postazioni di lavoro.

3. Non vengono installate apparecchiature specificamente preordinate al controllo a distanza dell'attività del personale universitario e di tutti coloro che operano a vario titolo nell'Università, non saranno 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.
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'articolo 4, comma 1, della legge n. 300/1970, sottoponendo in via preventiva il progetto di installazione dei sistemi alle rappresentanze sindacali e, in mancanza di raggiungimento di un accordo, presentando istanza all'Ispettorato del lavoro.

Articolo 6 – Conservazione

1. Le immagini acquisite dalle unità di ripresa sono visualizzate su monitor collocati nei locali della portineria ove sono situate le postazioni di controllo. L'accesso ai locali portineria è consentito in via ordinaria, al Designato, agli Incaricati, al personale di pubblica sicurezza o di polizia giudiziaria, al personale adibito al servizio di portierato e pulizia. L'accesso di soggetti diversi da quelli indicati può avvenire solo in via eccezionale, per comprovata necessità in relazione alle finalità indicate nell'articolo 3 e previa autorizzazione del Titolare o del Designato.

2. Le immagini sono conservate su appositi server o supporti analoghi custoditi nel rispetto delle misure di sicurezza richieste dalla vigente normativa.

3. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nel qual caso la conservazione verrà estesa a settantadue ore, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria o di Polizia Giudiziaria.

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, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Articolo 7 - Misure di sicurezza

I dati personali oggetto di trattamento sono conservati ai sensi e per gli effetti del precedente art. 10.
I dati raccolti mediante il sistema di videosorveglianza sono protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, 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 al fine di garantire la sicurezza del trattamento.
Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Università terrà 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'Università stessa.
A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:
a) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato al precedente art. 10, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
b) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele: in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
c) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
d) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà 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.
Il Titolare ed il Designato vigilano sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvedono altresì 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.

Articolo 8 – Cancellazione

1. Le immagini registrate vengono cancellate automaticamente da ogni supporto allo scadere del termine di conservazione stabilito ai sensi dell'art. 6 del presente Regolamento, con sovra-registrazione e modalità che rendono inutilizzabili i dati cancellati; tale impostazione dei sistemi non è tecnicamente modificabile.

Articolo 9 – Accesso ai dati

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 all'art. 4 del presente Regolamento.
L'accesso alle immagini è consentito esclusivamente:
a) al Titolare, al Designato, agli eventuali Responsabili ed agli incaricati del trattamento;
b) 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

ovvero, in casi del tutto eccezionali, all'amministratore di sistema dell'Università (preventivamente individuato quale incaricato del trattamento dei dati);
c) 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. 12. 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, dovrà pertanto essere utilizzata, da parte del Titolare del trattamento, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti;
d) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90, l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. 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.
Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito "registro degli accessi" (cartaceo od informatico), conservato a cura del Designato, nel quale sono riportati ad opera degli incaricati:

- la data e l'ora dell'accesso;
- l'identificazione del terzo autorizzato;
- i dati per i quali si è svolto l'accesso;
- gli estremi e la motivazione dell'autorizzazione all'accesso;
- le eventuali osservazioni dell'incaricato;
- la sottoscrizione del medesimo.

Articolo 10 - 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 o, nei casi previsti dalla legge, di regolamento. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali, previa comunicazione al Garante nei termini e con le modalità previste all'art. 2-ter, comma 2, del D.Lgs. n. 196/2003.
2. Sono fatte salve in ogni caso la comunicazione e la diffusione di 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.
3. La comunicazione e la diffusione devono essere in ogni caso autorizzate dal Titolare del trattamento ai sensi dell'art. 4 del presente Regolamento.
4. I dati non sono in nessun caso soggetti a diffusione generalizzata.

Articolo 11 - Informativa agli interessati

1. 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 semplificato di informativa "minima", indicante il Titolare del trattamento e le finalità perseguite, riportato in fac-simile nell'allegato n. 1 al Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010.
2. L'informativa deve essere collocata prima del raggio di azione della videocamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, potranno essere installati più cartelli informativi.
3. L'Università mette a disposizione degli interessati sul proprio sito internet, mediante affissione in bacheche e presso gli sportelli destinati agli utenti, il testo completo dell'informativa, contenente tutti gli elementi di cui agli artt. 13 e 14 RGPD.

Articolo 12 - Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, 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 di cui all'art. 17 RGPD, 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, ai sensi dell'art. 21, RGPD.
L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Università, ai sensi dell'art. 38, paragrafo 4, RGDP (i cui dati di contatto sono disponibili sul sito istituzionale dell'Università nella sezione "Privacy") ovvero al Designato o direttamente al Titolare.
Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
- il luogo, la data e la fascia oraria della possibile ripresa;
- l'abbigliamento indossato al momento della possibile ripresa;
- gli eventuali accessori in uso al momento della possibile ripresa;
- l'eventuale presenza di accompagnatori al momento della possibile ripresa;
- l'eventuale attività svolta al momento della possibile ripresa;
- eventuali ulteriori elementi utili all'identificazione dell'interessato.

Il Designato accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.
Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.
I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.
Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Articolo 13 - Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, RGPD e al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.

Articolo 14 - Entrata in vigore

Il presente Regolamento è adottato con decreto rettorale ed entra in vigore il 1.8.2019.

Bergamo, 25.7.2019

IL RETTORE
F.to Prof. Remo Morzenti Pellegrini

ALLEGATO

Informativa sul trattamento dei dati personali connessi all'utilizzo di sistemi di Videosorveglianza ai sensi dell'articolo 13 del Regolamento UE 2016/679 (di seguito GDPR)

Informazioni sul trattamento dei dati personali connessi all'utilizzo di sistemi di Videosorveglianza ai sensi dell'articolo 13 del Regolamento UE 2016/679 (di seguito GDPR)

L'Università degli Studi di Bergamo, in qualità di titolare del trattamento informa, che tratterà i Suoi dati personali (come definiti all'art. 4(1) del Regolamento) utilizzando i sistemi di videosorveglianza installati presso le sedi di Via …… e …… in base a quanto previsto dal Regolamento (UE) 2016/679 – GDPR, dal D.Lgs. 196/2003 così come modificato dal D.Lgs. 101/2018 e dal Provvedimento del Garante per la protezione dei dati personali in materia di videosorveglianza dell'8 aprile 2010. La presente informativa integra l'informativa "semplificata" fornita attraverso i cartelli posti in corrispondenza delle nostre telecamere.

Titolare e Responsabile della Protezione dei Dati

Il Titolare del trattamento è l'Università degli Studi di Bergamo, di seguito Università, con sede in via Salvecchio, 19 - 24129 Bergamo. L'Università ha nominato un Responsabile della Protezione dei Dati (RPD o DPO) disponibile all'indirizzo dpo@unibg.it per qualunque informazione inerente il trattamento dei Suoi dati personali da parte dell'Università.

A. DATI PERSONALI RACCOLTI

I dati personali che La riguardano, raccolti e trattati dall'Università, sono le immagini rilevate attraverso il sistema di videosorveglianza attualmente in uso.

B. FINALITÀ, BASE GIURIDICA E MODALITÀ DEL TRATTAMENTO

Il trattamento dei dati personali che la riguarda è necessario per garantire la sicurezza e la tutela del patrimonio, nonché l'incolumità e la sicurezza degli studenti e delle persone che svolgono le proprie mansioni presso il Titolare.

La base giuridica del trattamento è costituita dal perseguimento del legittimo interesse del Titolare (art.6(1)(f) del Regolamento).

In relazione alle finalità sopra indicate, il trattamento dei Suoi dati avverrà nel rispetto dei principi di liceità, correttezza, trasparenza, adeguatezza, pertinenza e necessità di cui all'art. 5, paragrafo 1 del Regolamento (UE), mediante strumenti manuali, informatici e telematici in modo pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono trattati e, comunque, in modo da garantire la massima sicurezza e riservatezza e sempre in piena conformità alla normativa vigente.

C. AMBITO DI CIRCOLAZIONE E COMUNICAZIONE DEI DATI

Per il perseguimento delle finalità sopra indicate, i Suoi dati personali saranno comunicati ai dipendenti e ai collaboratori del Titolare, che operano in qualità di incaricati dell'esecuzione del presente trattamento, autorizzati in funzione del proprio profilo.

I suoi dati personali potranno essere comunicati a persone fisiche o giuridiche che collaborano con l'Università per il perseguimento delle finalità sopra indicate. Questi soggetti svolgeranno la funzione di responsabile del trattamento dei dati ai sensi e per gli effetti dell'art. 28 del Regolamento, oppure opereranno in totale autonomia come autonomi titolari del trattamento.

Le immagini non saranno in alcun modo comunicate o diffuse a terzi, se non per rispondere a eventuali richieste da parte di Organi di Polizia o dell'Autorità Giudiziaria.

D. CONSERVAZIONE ED EVENTUALE TRASFERIMENTO DEI DATI PERSONALI

I Suoi dati personali saranno conservati presso l'Università nel rispetto dei tempi di conservazione stabiliti dalla legge, nello specifico per 72 ore dalla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura degli uffici, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa. Dopo tale periodo, si provvederà alla cancellazione delle stesse mediante sovrascrittura.

I dati personali non saranno trasferiti a un paese terzo o ad un'organizzazione internazionale.

E. I SUOI DIRITTI

L'interessato (soggetto ripreso) ha il diritto di chiedere al Titolare, in qualunque momento, l'accesso ai suoi dati personali o la cancellazione degli stessi o di opporsi al loro trattamento, ha diritto di richiedere la limitazione del trattamento nei casi previsti dall'art. 18 del Regolamento, nonché di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati che la riguardano, nei casi previsti dall'art. 20 del Regolamento. Trattandosi di dati trattati tramite il sistema di videosorveglianza, non è in concreto esercitabile il diritto di rettifica e integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

I diritti possono essere esercitati rivolgendosi via e-mail al Titolare del trattamento al seguente indirizzo di posta elettronica: privacy@unibg.it

Ai sensi della Normativa Applicabile, l'interessato ha in ogni caso il diritto di proporre reclamo all'autorità di controllo competente (Garante per la Protezione dei Dati Personali) qualora ritenesse che il trattamento dei suoi Dati Personali sia contrario alla normativa vigente.