



REGOLAMENTO SULL'USO DI STRUMENTI DI VIDEOSORVEGLIANZA DELL'UNIVERSITÀ DI FERRARA

Emanato con Decreto Rettorale Rep. n. 1263/2025 Prot. n. 255709 del 28/07/2025

Entrata in vigore: 14 agosto 2025

Art. 1 Definizioni	1
Art. 2 Oggetto	2
Art. 3 Principi generali	2
Art. 4 Finalità	3
Art. 5 Tutela dei lavoratori	3
Art. 6 Titolare del trattamento	4
Art. 7 Responsabili del trattamento	4
Art. 8 Autorizzati al trattamento	4
Art. 9 Sicurezza dei dati	4
Art. 10 Dislocazione dei sistemi di videosorveglianza	4
Art. 11 Conservazione dei dati	5
Art. 11 Cancellazione dei dati	5
Art. 12 Divieto di comunicazione e diffusione dei dati	5
Art. 13 Informativa	5
Art. 14 Diritti dell'interessato	6
Art. 15 Norme di rinvio	6
Art. 16 Entrata in vigore	6

Articolo 1 - Definizioni

Al fine del seguente regolamento si intende per:

- a) "Università" o "Ateneo", l'Università degli Studi di Ferrara;
- b) "GDPR", 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);

- c) “Codice Privacy”, il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento UE n. 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);
- d) “Provvedimento 8 aprile 2010 del Garante”, la Deliberazione 8 aprile 2010 del Garante per la protezione dei dati personali “Provvedimento in materia di videosorveglianza”, pubblicato sulla Gazzetta Ufficiale n. 99 del 29 aprile 2010);
- e) “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);
- f) “Garante”, il Garante per la protezione dei dati personali;
- g) “Titolare”, il Titolare del trattamento ai sensi dell'art. 4, n. 7), del GDPR, e cioè 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;
- h) “Responsabile”, il Responsabile del trattamento ai sensi dell'art. 4, n. 8), del GDPR, e cioè il soggetto esterno, persona fisica o giuridica, autorità pubblica o altro organismo che tratta i dati personali per conto del titolare del trattamento;
- i) “DPO” o “Responsabile per la protezione dei dati”, la persona fisica o giuridica con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, designata dal Titolare e dal Responsabile del trattamento per assolvere i compiti di cui all'articolo 39 del GDPR;
- j) “Incaricati” o “autorizzati”, le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- k) “Interessato”, la persona fisica i cui dati personali sono oggetto di trattamento.

Articolo 2 - Oggetto

1. Il presente Regolamento disciplina l'utilizzo dei sistemi di videosorveglianza attivati presso le strutture, aree di pertinenza e sedi dell'Università degli Studi di Ferrara ed il trattamento dei dati personali acquisiti attraverso i medesimi sistemi, in conformità alle disposizioni del GDPR, dello Statuto dei lavoratori, del Codice Privacy, del Provvedimento 8 aprile 2010 del Garante, nonché agli inerenti provvedimenti ed atti interpretativi e di indirizzo.
2. Tutte le cariche, professioni e titoli inerenti a funzioni nominate nel presente regolamento e declinate al genere maschile devono intendersi riferite anche al corrispondente termine di genere femminile.

Articolo 3 - Principi generali

1. Il trattamento dei dati personali effettuato attraverso i sistemi di videosorveglianza all'interno o in prossimità delle strutture dell'Università avviene esclusivamente nell'ambito dello svolgimento delle attività istituzionali e in forza dei legittimi interessi dell'Ateneo, del personale e dell'utenza.
2. L'installazione e l'utilizzo dei sistemi di videosorveglianza ed il trattamento dei dati personali acquisiti mediante gli stessi avvengono nel rispetto dei diritti e delle libertà fondamentali degli interessati, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.
3. Il trattamento dei dati personali viene effettuato in osservanza dei seguenti principi:
 - a) principio di legalità: l'installazione dei sistemi di videosorveglianza e il successivo trattamento dei dati personali avviene nel rispetto della normativa vigente in materia;
 - b) principio di necessità: i sistemi informatici sono configurati in modo tale da utilizzare dati personali esclusivamente nel caso in cui il trattamento sia necessario per il perseguimento delle finalità di cui al successivo articolo 4;
 - c) principio di proporzionalità: la dislocazione delle videocamere e le modalità di ripresa sono effettuate in modo da comportare esclusivamente il trattamento di dati pertinenti e non eccedenti alle finalità perseguite;
 - d) 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.

Articolo 4 - Finalità

1. L'Università si avvale di sistemi di videosorveglianza esclusivamente per il perseguimento delle seguenti finalità:
 - a) favorire la sicurezza e l'incolumità di studenti, personale universitario, collaboratori, fornitori e visitatori a qualunque titolo dell'Ateneo, che accedono alle strutture, aree di pertinenza o sedi universitarie;
 - b) tutelare il patrimonio mobiliare e immobiliare, di proprietà o in gestione all'Università, da atti vandalici, furti e danneggiamenti;
 - c) tutelare il patrimonio mobiliare di terzi che accedono alle strutture, aree di pertinenza o sedi universitarie;
 - d) tutelare il patrimonio informativo e di dati dell'Università;
 - e) monitorare e controllare gli accessi ad aree non aperte al pubblico e riservate a personale autorizzato dall'Università;
 - f) cooperare alla tutela dell'ordine e della sicurezza pubblica ed alla rilevazione, alla prevenzione e all'accertamento di illeciti a danno dell'Ateneo e dei terzi che accedono alle strutture, aree di pertinenza o sedi universitarie.

Articolo 5 - Tutela dei lavoratori

1. I sistemi di videosorveglianza non possono essere utilizzati dall'Ateneo per effettuare controlli a distanza sull'attività lavorativa o, in questo caso, dallo stesso utilizzati in eventuali contenziosi di lavoro nei confronti del personale universitario e di tutti coloro che operano a vario titolo in Ateneo, in conformità a quanto previsto dallo Statuto dei Lavoratori. Laddove, dai sistemi installati per le finalità sopra elencate (art. 4), derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, l'Università adotta le garanzie previste dall'art. 4 dello Statuto dei Lavoratori, stipulando un accordo con le rappresentanze sindacali dell'Ateneo.
2. In mancanza di accordo, gli impianti e gli strumenti di videosorveglianza possono essere installati solamente previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro.

Articolo 6 - Titolare del trattamento

1. Il Titolare del trattamento dei dati personali raccolti con i sistemi di videosorveglianza è l'Università degli Studi di Ferrara ai sensi degli artt. 24 e seguenti del GDPR.

Articolo 7 - Responsabili del trattamento

1. 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.
2. Tali soggetti vengono designati dal Titolare quali Responsabili del trattamento, ai sensi dell'art. 28 del GDPR, mediante contratto o altro atto giuridico, preliminarmente all'avvio delle attività o dei servizi ad essi affidati.

Articolo 8 - Autorizzati al trattamento

1. Ai sensi dell'art. 32 del GDPR e dell'art. 2-quaterdecies del Codice Privacy, l'Università 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.
2. L'Università individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
3. Agli incaricati sono attribuiti diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite al singolo operatore, distinguendo tra incaricati unicamente abilitati a visionare le immagini e incaricati che, a determinate condizioni, possono effettuare operazioni ulteriori.
4. Gli incaricati autorizzati all'attività di televigilanza prendono visione delle immagini esclusivamente in tempo reale.
5. Quando sono necessari interventi di manutenzione, gli operatori possono accedere alle immagini registrate esclusivamente per verifiche tecniche degli apparati di videoregistrazione. La visione delle immagini videoregistrate avviene alla presenza di un incaricato del trattamento.

Articolo 9 - Sicurezza dei dati

1. L'attività di videosorveglianza deve essere svolta nel rispetto del principio di protezione dei dati fin dalla progettazione e per impostazione predefinita delle modalità del trattamento, ai sensi degli artt. 25 e 32 del GDPR, in modo tale da prevenire, mediante l'adozione di idonee misure di sicurezza, i rischi di accesso, distruzione, perdita, modifica e divulgazione non autorizzata, accidentale o illegale, dei dati trattati.

Articolo 10 - Dislocazione dei sistemi di videosorveglianza

1. L'individuazione dei sistemi di videosorveglianza dell'Università viene riportata in appositi documenti custoditi dall'ufficio preposto alla manutenzione.

Articolo 11 - Conservazione e cancellazione dei dati

1. Le immagini registrate possono essere conservate per un periodo di tempo non superiore ai 7 giorni successivi alla loro rilevazione, decorsi i quali devono essere automaticamente cancellate.

Tale termine viene stabilito al fine di garantire la possibilità di procedere all'accertamento di illeciti a danno dell'Ateneo e dei terzi che accedono alle strutture, aree di pertinenza o sedi universitarie, tenendo conto della chiusura delle strutture nei fine settimana o in periodi festivi più lunghi.

2. Decorso il termine di conservazione dei dati di cui al comma precedente, le immagini registrate saranno automaticamente cancellate dai relativi supporti, in modo tale da renderne impossibile il recupero.
3. Rimangono salve speciali esigenze di ulteriore conservazione connesse a festività o periodi di chiusura delle sedi universitarie, o a specifiche richieste di autorità giudiziaria o polizia giudiziaria, per finalità di prevenzione, accertamento o repressione di reati.

Articolo 12 - Divieto di comunicazione e diffusione dei dati

1. Sono vietate la comunicazione e la diffusione delle immagini registrate a soggetti non autorizzati.
2. I dati possono essere comunicati a soggetti pubblici legittimati a richiederli, quali ad esempio l'Autorità giudiziaria e l'Autorità di pubblica sicurezza.
3. In caso di raccolta di immagini di fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza o dell'ordine pubblico, l'Università è tenuta a darne tempestiva comunicazione all'autorità giudiziaria.
4. I dati non possono essere oggetto di comunicazione a soggetti terzi diversi da quelli di cui ai commi precedenti e, in ogni caso, ad esclusione dei casi in cui la comunicazione sia necessaria all'adempimento di un obbligo di legge.

Articolo 13 - Informativa

1. L'Università informa gli interessati che stanno per accedere ad una zona videosorvegliata anche attraverso l'utilizzo di cartelli riportanti il modello semplificato di informativa, reso disponibile dal

Garante all'interno del proprio sito istituzionale, da redigere con l'indicazione del Titolare del trattamento, del Responsabile della protezione dati e delle finalità perseguite.

2. L'informativa è collocata prima del raggio di azione della videocamera con un formato ed un posizionamento tali da essere chiaramente visibile anche in condizioni di scarsa o insufficiente illuminazione ambientale, ad esempio quando il sistema di videosorveglianza sia attivo in orario notturno.
3. In presenza di più videocamere e in relazione alla vastità delle aree oggetto di rilevamento, l'informativa è resa mediante affissione di una pluralità di cartelli.
4. L'Università mette a disposizione degli interessati sul proprio sito istituzionale, nella sezione "Protezione dati personali", il testo completo dell'informativa di cui all'art. 13 del GDPR.

Articolo 14 - Diritti dell'interessato

1. L'interessato al trattamento, ossia la persona che ritiene di essere stata ripresa, può esercitare nei confronti dell'Università tutti i diritti previsti dagli articoli 15 e seguenti del GDPR.
2. Non è in concreto esercitabile il diritto di aggiornamento o integrazione, nonché il diritto di rettifica di cui all'articolo 16 del GDPR in considerazione della natura intrinseca dei dati trattati (immagini raccolte in tempo reale riguardanti un fatto obiettivo).
3. Non è esercitabile il diritto alla portabilità dei dati di cui all'articolo 20 del GDPR in quanto le immagini acquisite con il sistema di videosorveglianza possono essere trasmesse limitatamente ai casi previsti dall'art. 12 del presente regolamento.
4. Per esercitare i propri diritti, gli interessati possono rivolgersi al Titolare del trattamento, o al DPO, utilizzando i contatti presenti nella sezione "Protezione dati personali" del portale dell'Ateneo, esibendo o allegando alla richiesta idonei documenti di riconoscimento. Il Titolare dovrà fornire una risposta tempestiva e comunque entro un mese dalla richiesta, estensibile fino a tre mesi in casi di particolare complessità.

Articolo 15 - Norme finali

1. Il presente Regolamento è emanato con decreto rettorale ed entra in vigore il 15° giorno successivo alla data di pubblicazione nell'Albo Online.
2. Per tutti gli aspetti non espressamente disciplinati dal presente regolamento, si rinvia alle normative comunitarie e nazionali vigenti ed ai provvedimenti e atti interpretativi e di indirizzo in materia di trattamento dei dati personali e di videosorveglianza.