TRATTAMENTO DEI DATI PERSONALI TRAMITE IMPIANTO DI VIDEOSORVEGLIANZA

- MANUALE OPERATIVO -

Università degli Studi di Trieste

INDICE

1. Scopo

- Lo scopo del presente manuale consiste nella definizione delle modalità operative da attuare per la progettazione, installazione, manutenzione e gestione degli impianti di videosorveglianza nel rispetto della disciplina in materia di protezione dei dati personali e in applicazione del Regolamento sul Trattamento dei dati personali tramite impianti di videosorveglianza dell'Università di Trieste approvato con Delibera del Consiglio di Amministrazione del 3 marzo 2023 e oggetto di specifico accordo sindacale.

2. Riferimenti normativi

- D. Lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" e s.m.i;
- Regolamento UE 679/2018 "GDPR";
- D.Lgs. 10 agosto 2018 n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- L. 20 maggio 1970 n. 300 (Statuto dei Lavoratori);
- Provvedimento del Garante per la protezione dei dati personali 8 aprile 2010 in materia di videosorveglianza;
- Linee guida 3/2019 European Data Protection Board sul trattamento dei dati personali attraverso dispositivi video.

3. Riferimenti regolamentazione Ateneo

- Regolamento in materia di protezione dei dati personali dell'Università approvato con Decreto Rettorale n. 514 di data 8/8/2019
- Regolamento sul Trattamento dei dati personali tramite impianti di videosorveglianza dell'Università di Trieste approvato con Delibera del Consiglio di Amministrazione del 3 marzo 2023
- Accordo sindacale sottoscritto in data 16 marzo 2023.

4. Principi e presupposti di liceità degli impianti

- In ossequio ai principi di liceità, necessità, proporzionalità, che implicano la limitazione delle finalità e la minimizzazione dei dati, di trasparenza e partecipazione di cui all'art. 5 GDPR, ogni procedura tesa all'installazione di impianti di videosorveglianza e la loro gestione sono svolti nel rispetto delle istruzioni e procedure previste nel presente manuale e del Regolamento sul Trattamento dei dati personali tramite impianti di videosorveglianza

dell'Università di Trieste approvato con Delibera del Consiglio di Amministrazione del 3 marzo 2023 (di seguito "Regolamento").

5. Progettazione degli impianti

- La progettazione degli impianti e la loro installazione deve rispettare i principi di privacy by design e privacy by default di cui all'art. 25 GDPR.
- Nella progettazione vengono individuate le misure alternative meno invasive per limitare l'utilizzo di telecamere, o per individuarne le funzionalità pertinenti (a titolo di esempio telecamere fisse o brandeggiabili, funzioni di zoom, funzioni di attivazione intelligente) e la loro dislocazione secondo il principio di necessità e proporzionalità.
- Nella progettazione vengono valutate, secondo il contesto, le funzioni di sola visualizzazione o registrazione delle immagini delle singole telecamere o di gruppi di telecamere, secondo il principio di minimizzazione.
- Nella progettazione vengono assunte tutte le misure tecniche e organizzative necessarie per evitare la raccolta di dati di particolari categorie di cui all'art. 9 GDPR.
- Nel rispetto del principio di minimizzazione e liceità sono evitate le installazioni di telecamere in zone quali i servizi igienici, le zone ristoro e in corrispondenza agli orologi marcatempo.
- È inoltre, esclusa l'installazione di telecamere all'interno dei locali nei quali si svolgono attività di didattica, studio e ricerca (aule didattiche e di studio, biblioteche e laboratori).
- Resta in ogni caso esclusa la possibilità di ripresa negli uffici/locali dove il personale universitario presta la propria attività lavorativa.
- È vietata l'installazione di telecamere finte o non funzionanti, nascoste o occulte.
- Nella scelta dei fornitori o nell'acquisto di dispositivi hardware e software, è necessario assicurare il rispetto dei requisiti previsti dal presente manuale nonché dalla disciplina applicabile in materia, al fine di assicurare la protezione dei dati personali al loro intero ciclo di vita.
- 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.

- Il progetto di impianto, prima dell'installazione, deve essere sottoposto ad analisi dei rischi con la seguente procedura utilizzando la check list di cui all'allegato 2 per rilevare eventuali vulnerabilità:

Azione	Funzione responsabile
Redazione analisi dei rischi	Area dei servizi tecnici e di supporto in collaborazione con il Responsabile interno richiedente e RUP
Parere	Responsabile per la protezione dei dati - DPO
Approvazione	Gruppo di supporto al Responsabile per la Protezione dei Dati

- I soggetti responsabili della redazione dell'analisi dei rischi curano l'applicazione di disposizioni specifiche di settore in materia di rispetto del diritto alla riservatezza, la ricerca di precedenti pronunce del Garante per la protezione dei dati personali in relazione a particolari prescrizioni inerenti impianti analoghi.

- Qualora l'analisi dei rischi evidenzi che le misure introdotte non consentono di mitigare un rischio elevato per la riservatezza, integrità e disponibilità dei dati o comunque il trattamento possa comportare un rischio elevato per i diritti e le libertà degli interessati ai sensi dell'art. 35 GDPR, viene effettuata una valutazione di impatto (DPIA) preliminare all'installazione dell'impianto.

  La Valutazione di impatto viene effettuata secondo la seguente procedura:

Azione	Funzione responsabile
Redazione DPIA	Area dei servizi tecnici e di supporto in collaborazione con il Gruppo di supporto al Responsabile per la Protezione dei Dati
Parere	Responsabile per la protezione dei dati - DPO
Approvazione formale	Legale rappresentante - Rettore

6. Documento di liceità

- Il documento di liceità dà conto dell'osservanza dei principi di cui al Regolamento e del presente manuale e costituisce il presupposto per la legittimità della progettazione e dell'acquisto di ciascun impianto di videosorveglianza e/o gruppo di telecamere.

- Il documento di liceità è redatto secondo il modello di cui all'Allegato 3.

- Il documento di liceità viene redatto secondo la seguente procedura:

Azione	Funzione responsabile
Effettuazione analisi del rischio/DPIA	Vedi par.5 del presente manuale
Redazione documento di liceità	Responsabile interno richiedente
Revisione documento di liceità	Area dei servizi tecnici e di supporto
Parere	Responsabile per la protezione dei dati - DPO
Approvazione	Gruppo di supporto al Responsabile per la Protezione dei Dati

7. Informazioni sul trattamento dei dati personali ex art. 13-14 GDPR

- Gli interessati devono essere informati del trattamento applicato ai loro dati personali in modo trasparente. Le informazioni di cui agli articoli 13-14 GDPR vengono fornite agli interessati su più livelli secondo le misure organizzative generali stabilite dal Titolare del trattamento e/o previste dal Regolamento e dal presente manuale.

- Gli interessati devono essere informati che stanno per accedere a un'area videosorvegliata tramite l'esposizione di cartelli di informativa c.d. "minima", utilizzando il modello di cui all'All. 1.

- I cartelli di informativa minima devono essere installati prima del raggio d'azione della telecamera, in modo tale che l'interessato possa facilmente riconoscere le circostanze della ripresa prima di entrare nell'area monitorata, e devono essere chiaramente visibili in ogni condizione atmosferica o di illuminazione ambientale.

- Il cartello di informativa c.d. minima rinvia al testo di informativa recante tutti i requisiti informativi di cui all'art. 13-14 GDPR mediante utilizzo di QR Code per l'accesso mediante dispositivi informatici o istruzioni per l'accesso alle informazioni in ambiente fisico. In entrambi i casi, le informazioni devono essere reperibili agevolmente da parte degli interessati, anche prima di entrare nel perimetro di ripresa delle telecamere.

- La liceità dei testi informativi viene valutata dal Titolare del trattamento secondo le misure generali per la gestione della protezione dei dati. L'installazione, manutenzione e aggiornamento dei cartelli e delle informative complete sono in capo ai soggetti individuati come segue:

Azione	Funzione responsabile

Installazione cartelli informativi	Area dei servizi tecnici e di supporto
Installazione informative complete in ambiente fisico (es. affissione presso reception o all'ingresso)	Area dei servizi tecnici e di supporto
Installazione informative complete in ambiente digitale (es. pubblicazione su sito web)	Area dei servizi tecnici in collaborazione con il Gruppo di supporto al Responsabile per la Protezione dei Dati
Aggiornamento testi informativi	Area dei servizi tecnici in collaborazione con il Gruppo di supporto al Responsabile per la Protezione dei Dati

8. Condizioni per l'attivazione dell'impianto

- Nessun impianto di videosorveglianza entra in funzione prima di:
  - effettuazione dell'analisi dei rischi e/o eventuale Valutazione di impatto (DPIA), come previsto dall'par.5 del presente manuale;
  - stipula dell'accordo sindacale o autorizzazione dell'Ispettorato del lavoro eventualmente necessari, come previsto dal Regolamento;
  - redazione del documento di liceità, secondo la procedura di cui al par. 6 del presente manuale;
  - applicazione delle misure tecniche e organizzative previste;
  - installazione dei cartelli informativi secondo modalità previste dal par.7 del presente manuale.

- Soddisfatti i requisiti suindicati, l'impianto entra in funzione a seguito di approvazione secondo la procedura di seguito indicata. La documentazione richiamata e gli ulteriori documenti inerenti l'impianto (schede tecniche, manuali di istruzioni, contratti con fornitori ecc.) vengono conservati per tutto il ciclo di vita dell'impianto.

Azione	**Funzione responsabile**
Approvazione attivazione impianto	Gruppo di supporto al Responsabile per la Protezione dei Dati
Conservazione documentazione accountability impianto	Area dei servizi tecnici

9. Ruoli e responsabilità nella gestione dell'impianto

- Nella fase di valutazione di liceità e analisi dei rischi di cui ai par. 5 e 6 del presente manuale viene valutato il ruolo e responsabilità dell'ente rispetto ai trattamenti di dati personali effettuati dall'impianto stesso e, in particolare, i trattamenti per i quali le operazioni di trattamento vengono effettuate in qualità di titolare del trattamento ai sensi dell'art. 24 GDPR, in qualità di contitolare del

trattamento ai sensi dell'art. 26 GDPR o in qualità di responsabile del trattamento ai sensi dell'art. 28 GDPR. Il documento di liceità di cui all'All. 3 individua i ruoli nel trattamento dei dati personali.

- Qualora l'installazione, gestione o manutenzione dell'impianto comporti la comunicazione di dati personali a soggetti terzi in qualità di contitolari del trattamento o responsabili del trattamento ai sensi dell'art. 28 GDPR, i contratti stipulati devono includere i requisiti previsti dal presente manuale, al fine di garantire il rispetto dello stesso livello di protezione dei dati personali durante il loro intero ciclo di vita.
- Nei casi di cui i paragrafi precedenti viene stabilito, durante la fase di analisi dei rischi, se sia necessario introdurre ulteriori misure di sicurezza rispetto a quanto previsto dal par. 15 del presente manuale, secondo il seguente modello:

Sistemi integrati di videosorveglianza	
Gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento con l'utilizzo delle medesime infrastrutture tecnologiche	
Limitazione, per ciascun titolare, al trattamento per le proprie finalità	XXXX
Registrazione accessi logici e operazioni effettuate sulle immagini, comprensivi di riferimenti temporali	XXXX
Indicazione del periodo di conservazione file di log	*(Almeno 6 mesi)*
Separazione delle immagini registrate dai diversi titolari	XXXX

Sistemi integrati di videosorveglianza	
Collegamento telematico di diversi titolari del trattamento ad un centro unico gestito da un soggetto terzo (es. società di vigilanza)	
Stipula del contratto del soggetto terzo in qualità di responsabile del trattamento ex art. 28 GDPR	XXXX
Misure tecniche e organizzative per impedire correlazione delle immagini raccolte per conto di ciascun titolare	XXXX
Registrazione accessi logici e operazioni effettuate sulle immagini, comprensivi di riferimenti temporali	*(Almeno 6 mesi)*

Indicazione del periodo di conservazione file di log	XXXX
Separazione delle immagini registrate dai diversi titolari	XXXX
Sistemi integrati di videosorveglianza	
Collegamento dell'impianto alle sale e centrali operative degli organi di polizia	
Utilizzo del modello di informativa n. 2 (All. 1) per rendere noto il collegamento.	XXXX
Registrazione accessi logici e operazioni effettuate sulle immagini, comprensivi di riferimenti temporali	XXXX
Indicazione del periodo di conservazione file di log	*(Almeno 6 mesi)*
Separazione delle immagini registrate dai diversi titolari	XXXX

10. Funzioni e obblighi dei soggetti designati interni

- Il Regolamento individua i soggetti designati ai sensi dell'art. 2 quaterdecies D.Lgs. 196/2003 con i compiti individuati nel presente manuale.
- I soggetti designati forniscono istruzioni ai soggetti autorizzati al trattamento dei dati personali secondo quanto indicato dal titolare del trattamento e verificano periodicamente l'adeguatezza e l'attualità delle istruzioni consegnate agli autorizzati.
- I soggetti designati monitorano le fasi di manutenzione dell'impianto da parte di soggetti esterni o le richieste di accesso e/o comunicazione da parte dell'autorità giudiziaria.
- I soggetti designati forniscono al titolare del trattamento informazioni su eventuali modifiche all'impianto o del contesto al fine di attivare le procedure di rivalutazione e aggiornamento di cui all'art. 17 del presente regolamento.

11. Autorizzazione al trattamento delle immagini in presa diretta o registrate

- Sono individuati soggetti autorizzati ai sensi dell'art. 29 GDPR con i compiti individuati nel presente regolamento.
- Ogni soggetto autorizzato riceve istruzioni in forma scritta secondo i modelli di cui agli All. 4-5, al fine di individuare i livelli di accesso, distinguendo per la sola visualizzazione delle immagini o accesso alle registrazioni, operazioni

autorizzate secondo il mansionario (accesso, duplicazione, modifica, cancellazione), e compiti rispetto al presente regolamento.

12. Periodo di conservazione dei dati e cancellazione

- Le immagini vengono conservate per il periodo strettamente necessario e proporzionale al perseguimento delle finalità indicate agli interessati.

Periodo di conservazione delle immagini*	
Telecamera o gruppo di telecamere	*Termine di durata*
Tutte	Periodo strettamente necessario e proporzionale al perseguimento delle finalità indicate agli interessati e comunque non superiore a quanto stabilito dal Regolamento

∗ Per particolari esigenze tecniche i tempi indicati potrebbero essere estesi, ad esempio in caso di festività o chiusura degli uffici o nel caso in cui sia necessario aderire a una richiesta dell'autorità giudiziaria.

13. Comunicazione a terzi

- Al di fuori dei casi previsti dal presente paragrafo e dal par. 9 del presente manuale non è possibile comunicare a terzi i dati personali trattati tramite l'impianto.

- In caso di richiesta di accesso o comunicazione dei dati da parte dell'autorità giudiziaria, tale operazione è sempre lecita se necessaria per l'assolvimento di un obbligo di legge. Il soggetto designato che riceve le richieste, prima di assistere l'autorità giudiziaria, chiede di documentare per iscritto tale richiesta e inoltra la documentazione al titolare del trattamento e al Responsabile per la protezione dei dati personali.

14. Esercizio dei diritti degli interessati

- I soggetti interessati possono esercitare i propri diritti secondo le procedure generali in materia predisposte dal titolare del trattamento.

- In caso di richieste di accesso o cancellazione dei dati, prima di dare riscontro alla richiesta, è necessario verificare la presenza di controinteressati il cui diritto alla riservatezza prevale rispetto ai diritti vantati dal soggetto richiedente.

15. Ulteriori misure di sicurezza tecniche e organizzative

- Oltre alle misure generali previste dal presente regolamento, ogni impianto deve rispettare le seguenti misure tecniche e organizzative fornendo evidenza della specifica soluzione adottata nell'analisi dei rischi:

Descrizione delle misure organizzative
Posizionamento dei monitor
Criterio di change management per concessione, modifica e revoca delle autorizzazioni
Criterio di configurazione dei diversi livelli di visibilità e trattamento delle immagini da parte degli operatori
Criterio di limitazione dei livelli di accesso alle immagini registrate in sincrono alla ripresa, in tempo differito, e effettuazione operazioni di cancellazione e duplicazione
Gestione della cancellazione automatica delle immagini
Cautele in caso di manutenzione all'impianto da parte di soggetti terzi
Inventario degli asset
Posizionamento e orientamento delle telecamere
Illuminazione delle telecamere e dei cartelli informativi
Coinvolgimento di Rappresentante dei lavoratori in occasione di estrazione delle immagini registrate
Registro degli accessi fisici

Descrizione delle misure tecniche
Sicurezza delle reti e delle comunicazioni
Memorizzazione delle immagini
Sicurezza fisica hardware
Disattivazione funzioni non necessarie
Oscuramento delle immagini o parte delle immagini
Limitazione dell'angolo visuale
Cifratura dei dati
Firewall e sistemi anti-intrusione
Controllo degli accessi fisici
Controllo degli accessi logici - credenziali
Controllo degli accessi logici - log
Monitoraggio degli eventi - log
Gestione della cancellazione automatica delle immagini

- In caso di particolari e documentate necessità potranno essere previsti livelli di sicurezza maggiori su impianti a protezione di ambienti ritenuti sensibili o che richiedano maggiore sorveglianza.

16. Gestione e manutenzione degli impianti di videosorveglianza

- Qualora un impianto di videosorveglianza sia gestito, anche solo parzialmente, inclusa la manutenzione, da soggetto esterno, si applica quanto previsto dal par.9 del presente manuale per l'individuazione di ruoli e responsabilità nel trattamento dei dati al fine di stipulare accordi scritti che garantiscano il livello di protezione previsto dal presente regolamento e dalla normativa applicabile rispetto allo stato dell'arte.

- Qualora un soggetto esterno debba accedere ai locali dell'ente o ad asset logici dell'impianto per finalità di manutenzione, l'ente adotta ogni misura tecnica o organizzativa necessaria per impedire al manutentore di effettuare trattamenti di dati personali. Qualora ciò non sia tecnicamente possibile per gli scopi della manutenzione, il soggetto designato interno richiede la sottoscrizione di una lettera di impegno alla riservatezza e sovrintende le operazioni di manutenzione per tutta la loro durata.

- Le credenziali di accesso all'impianto non vengono mai cedute o assegnate, nemmeno temporaneamente, a soggetti esterni per finalità di manutenzione.

17. Rivalutazione e aggiornamento

- L'area servizi tecnici aggiorna periodicamente il documento di liceità sulla base di nuove analisi del rischio, formulando le conseguenti proposte di conferma o di adeguamento, in termini di mantenimento, rafforzamento, ridimensionamento o modificazione dell'impianto.

- L'ufficio internal audit tramite aggiornamento periodico ed anche a campione verifica l'applicazione delle misure previste dal presente manuale.

Allegato 1. Modello grafico cartello videosorveglianza

Modello di cartello informativa c.d minima senza connessione a sistemi esterni

INFORMATIVA AI SENSI ART. 13 REGOLAMENTO EUROPEO 679/2016

LOGO TITOLARE DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO:
Università degli Studi di Trieste

Dati di contatto:
Sede legale XXX
Tel. XXX

Inserire email privacy

Le telecamere riprendono e registrano le immagini **fino a** XXX **ore.**

Il trattamento è effettuato per in esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e, in particolare, delle seguenti finalità:

- garantire la sicurezza e l'incolumità di studenti, personale, collaboratori, fornitori e visitatori a qualunque titolo dell'Università, che accedono alle strutture, aree di pertinenza o sedi di pertinenza;
- tutelare il patrimonio mobiliare e immobiliare, di proprietà o in gestione dell'Università, da atti vandalici, furti e danneggiamenti;
- cooperare alla tutela dell'ordine e della sicurezza pubblica ed alla rilevazione, alla prevenzione e all'accertamento di illeciti;
- beneficiare dell'azione deterrente, insita nei sistemi di sorveglianza.

INSERIRE QUI QR CODE A PAGINA SITO WEB UNITS "PRIVACY"

Per leggere l'informativa completa ai sensi dell'art. 13 GDPR sul trattamento dei dati personali accedere al seguente indirizzo: **inserire link** o consultare il testo affisso presso XXX/URP.

DIRITTI DEGLI INTERESSATI:

Come soggetto interessato puoi esercitare i tuoi diritti, in particolare il diritto di chiedere l'**accesso**, l'**opposizione** o la **cancellazione** dei tuoi dati.
Per esercitare i tuoi diritti contatta il titolare del trattamento e leggi l'informativa completa seguendo le istruzioni a sinistra.

Modello di cartello informativa c.d minima con connessione a sistemi esterni

INFORMATIVA AI SENSI ART. 13 REGOLAMENTO EUROPEO 679/2016

LOGO TITOLARE DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO:
DENOMINAZIONE

Dati di contatto:
Sede legale XXX
Tel. XXX

Inserire email privacy@...

Le telecamere riprendono e registrano le immagini **fino a** XXX **ore.**

Le immagini sono comunicate a XXX.

Il trattamento è effettuato per

- **necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.**

INSERIRE QUI QR CODE A PAGINA SITO WEB UNITS "PRIVACY"

Per leggere l'informativa completa ai sensi dell'art. 13 GDPR sul trattamento dei dati personali accedere al seguente indirizzo: **inserire link** o consultare il testo affisso presso XXX/URP.

DIRITTI DEGLI INTERESSATI:

Come soggetto interessato puoi esercitare i tuoi diritti, in particolare il diritto di chiedere l'**accesso**, l'**opposizione** o la **cancellazione** dei tuoi dati.
Per esercitare i tuoi diritti contatta il titolare del trattamento e leggi l'informativa completa seguendo le istruzioni a sinistra.

Allegato 2. Check list controlli

Domanda	Risposta
Dove sono posizionati i cartelli recanti l'informativa breve?	
Dove sono collocate le telecamere? Allegare prospetto se presente	
I cartelli sono collocati prima del raggio d'azione della telecamera?	
Il posizionamento dei cartelli è tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno?	
Descrivere le caratteristiche delle telecamere (es. fisse; speed dome; rilevamento infrarossi; sensore di movimento ecc). Allegare le schede tecniche.	
All'interno è presente il testo dell'informativa privacy estesa (es. affissa al muro)?	
Chi sono i soggetti che accedono alle immagini live?	
Chi sono i soggetti che accedono alle immagini registrate?	
In caso di accesso alle immagini registrate viene coinvolto il Rappresentante dei Lavoratori (RLS)?	
In caso di richiesta da parte della Polizia, chi sono i soggetti che estraggono le immagini?	
Sono previste credenziali di accesso per la visualizzazione delle immagini?	
Le credenziali di accesso consentono di effettuare solo le operazioni di propria competenza (visione live, visione registrazione, estrazione...)?	
I soggetti che accedono all'impianto hanno ricevuto istruzioni e incarico scritto?	

Quali sono i controlli di accesso alle immagini? Sono previsti meccanismi di autenticazione forte per esempio con doppia chiave logica tenuta da soggetti diversi?	
Come sono configurati i diversi livelli di visibilità e trattamento delle immagini?	
E' possibile cancellare manualmente le immagini?	
E' possibile duplicare le immagini?	
E' possibile limitare alcune operazioni (visualizzazione registrazioni, cancellazione, duplicazione) ad alcuni soggetti?	
Qual è il periodo di cancellazione delle immagini?	
La cancellazione delle immagini è automatica?	
Come avviene la cancellazione delle immagini? Descrivere ad es. modalità di sovrascrittura	
Le forze di polizia hanno un collegamento diretto all'impianto?	
L'impianto è collegato a reti informatiche interne?	
Qualora l'impianto sia collegato a reti informatiche, quali misure sono adottate per evitare accessi abusivi alle immagini?	
Le immagini vengono trasmesse dalle telecamere all'impianto attraverso rete pubblica o privata?	
In caso di rete pubblica, quali misure sono applicate per garantire la riservatezza della comunicazione?	
Sono applicate misure di crittografia nella comunicazione dei dati?	
L'impianto è collegato con altri impianti/sedi del Titolare del trattamento?	

L'impianto è collegato a società esterne (es. società di vigilanza, fornitori servizi videosorveglianza altro)? Quali?	
Se l'impianto è collegato a altri soggetti esterni, indicare una descrizione dell'impianto (es. centrale operativa, strutture tecnologiche separate, stessa struttura tecnologica...)	
Sono registrati gli accessi logici dei soggetti autorizzati?	
Sono registrati i log delle operazioni effettuate sulle immagini?	
Sono salvati i riferimenti temporali dei file di log?	
Per quanto tempo vengono salvati i log e i riferimenti temporali?	
Le immagini sono archiviate nel server o su impianto DVR dedicato?	
Indicare misure di sicurezza fisica applicate al server/impianto DVR	
I monitor dove sono collocati? Sono visibili anche a personale non autorizzato?	
L'impianto è stato oggetto di accordo sindacale? Se si allegare l'autorizzazione o l'accordo.	
Sono state valutate alternative, in modo documentabile, per conseguire le finalità senza installare le videocamere?	
Sono state documentate le esigenze che hanno determinato l'installazione dell'impianto? (es. precedenti furti, fatti di cronaca, ubicazione della struttura in luogo non sicuro, altro).	
Sono presente telecamere finte o non funzionanti?	

Allegato 3. Modello documento di liceità

DOCUMENTO DI LICEITÀ

Data prima redazione	Numero identificativo e ultima versione	Data ultima versione
XXX	XXX	XXX

Identificazione impianto	
Codice impianto/denominazione sintetica	XXX

Procedura di redazione	
Azione	**Funzione responsabile**
Effettuazione analisi del rischio/DPIA	XXXX
Redazione documento di liceità	XXXX
Revisione documento di liceità	XXXX
Parere	Responsabile per la protezione dei dati - DPO
Approvazione	XXXX

Con il presente documento si indicano le ragioni sottese alla scelta di utilizzare ciascun impianto di videosorveglianza con le rispettive tecnologie, evidenziandone la coerenza rispetto ai principi di:

- LICEITA', CORRETTEZZA E TRASPARENZA nei confronti dell'interessato;
- LIMITAZIONE DELLA FINALITÀ, ovvero dati raccolti e coerentemente trattati per finalità determinate, esplicite e legittime;
- MINIMIZZAZIONE DEI DATI, ovvero raccolta e trattamento secondo criteri di adeguatezza, pertinenza e necessità;
- ESATTEZZA dei dati anche rispetto alla finalità;
- LIMITAZIONE DELLA CONSERVAZIONE, coerente con le finalità per le quali i dati sono raccolti;
- INTEGRITA' E RISERVATEZZA, attraverso l'individuazione e l'applicazione di idonee misure di sicurezza tecniche ed organizzative.

Quanto di seguito descritto dà conto dell'avvenuta valutazione di natura, ambito di applicazione, contesto e finalità del trattamento in relazione alla valutazione del rischio di cagionare danni fisici, materiali o immateriali alle persone i cui dati vengono raccolti e trattati.

Ruoli nel trattamento dei dati	
Titolare del trattamento	XXX
Contitolare del trattamento	XXX
Responsabili del trattamento	XXX

Finalità del trattamento specifiche e base giuridica	
Legittimo interesse del titolare alla sicurezza del patrimonio aziendale	XXX
Legittimo interesse del titolare per esigenze organizzative e produttive	XXX
Legittimo interesse del titolare per la sicurezza sul lavoro	XXX
Legittimo interesse del titolare per l'accertamento, l'esercizio o la difesa dei propri diritti in sede giudiziaria	XXX
Necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri	XXX Esempi ❏ garantire la sicurezza e l'incolumità di studenti, personale, collaboratori, fornitori e visitatori a qualunque titolo dell'Università, che accedono alle strutture, aree di pertinenza o sedi di pertinenza; ❏ tutelare il patrimonio mobiliare e immobiliare, di proprietà o in gestione dell'Università, da atti vandalici, furti e danneggiamenti; ❏ cooperare alla tutela dell'ordine e della sicurezza pubblica ed alla rilevazione, alla prevenzione e all'accertamento di illeciti; ❏ beneficiare dell'azione deterrente, insita nei sistemi di sorveglianza.

Motivazione estesa e richiamo della documentazione a supporto
XXX Esempi ❑ Indicatori di insicurezza (denunce, furti, scippi, rapine, atti vandalici, danneggiamenti, incidenti stradali, situazioni problematiche nella viabilità urbana) ❑ Localizzazione degli eventi sul territorio limitrofo per individuare le aree di criticità ❑ Indicazioni della cittadinanza in relazione ad aree di cui è percepita l'insicurezza ❑ Orari di maggior rischio ❑ Strumenti tecnologici e risorse umane che l'ente può impiegare ❑ Razionalizzazione delle risorse ❑ Disponibilità finanziarie e riferimenti a potenziali, specifiche fonti di finanziamento

Motivazione dell'installazione
Sintesi dei motivi per cui l'impianto di videosorveglianza non può essere sostituito da interventi di vigilanza meno invasivi (le soluzioni alternative devono cioè risultare insufficienti o inattuabili).

Rivalutazione
All'esito del monitoraggio annuale/biennale/triennale/quadriennale/quinquennale, l'impianto ed i trattamenti di dati personali che ne derivano dovranno essere rivalutati a contesto giustificativo aggiornato. Sulla base della valutazione saranno individuate conseguenti misure, quali l'eliminazione, il riposizionamento, il rafforzamento o la conferma dell'impianto stesso.

Elenco allegati
❑ Planimetrie ❑ Manuali ❑ Schede tecniche ❑ Autorizzazioni e/o accordi sindacali ❑ Altro

Allegato 4. Modello lettera istruzioni soggetto autorizzato (solo visualizzazione)

MODELLO DI ISTRUZIONI DA INTEGRARE IN LETTERA DI AUTORIZZAZIONE SU FAC SIMILE UNIVERSITA' A SECONDA DELL'IMPIANTO E DEL PROFILO DI AUTORIZZAZIONE.

In caso di nomina a Responsabile del Trattamento, il fornitore è tenuto a dare istruzioni ai propri soggetti autorizzati secondo il seguente modello.

Il trattamento di immagini avviene secondo normativa applicabile di legge.
Lei verificherà che il trattamento delle immagini rilevate dai sistemi di videosorveglianza vengano trattate nel rispetto della protezione dei dati personali, e in particolare:

- che in ogni circostanza le azioni eseguite che comportano trattamento dei dati personali devono essere limitate a quanto strettamente necessario in relazione al perseguimento delle finalità dell'impianto e con i limiti qui indicati;
- che sia rispettato l'obbligo di massima riservatezza in relazione a qualsiasi informazione o dato personale acquisito;
- la password di accesso al monitor è personale, riservata e non cedibile;
- le persone non autorizzate alla visione delle immagini non possono accedere al locale in cui sono collocati i monitor. A tale scopo andrà affisso apposito cartello recante il divieto sulla porta del locale; tale divieto dovrà essere fatto valere nei confronti di chiunque;
- i monitor devono essere orientati in modo da escludere la visione anche accidentale delle immagini a persone non autorizzate che si trovino all'esterno del locale;
- il locale in cui sono collocati i monitor non può essere mai lasciato incustodito; in caso di allontanamento la porta di accesso deve essere chiusa a chiave;
- le operazioni diverse dalla visione sulle immagini, quali la copia, la modifica, la cancellazione, la comunicazione, la divulgazione o altro trattamento delle immagini con qualsiasi mezzo, sono vietate;
- la comunicazione dei dati personali acquisiti attraverso la visione delle immagini è consentita esclusivamente al referente interno;
- la diffusione dei dati personali acquisiti attraverso la visione delle immagini è vietata senza eccezioni;
- i monitor devono essere spenti dall'utente alla cessazione del proprio turno di servizio.

Lei è autorizzato alla sola visione in tempo reale delle immagini risultanti dai monitor ubicati in_____.
Nei casi in cui pervengano richieste formali di estrazione delle immagini registrate, scritte e firmate, lei non è autorizzato all'accesso e all'estrazione delle stesse.
L'unico soggetto autorizzato all'attività di estrazione delle immagini videoregistrate presso la sede legale è_____, che lei ha l'obbligo di informare tempestivamente.
Nel caso in cui una telecamera si dovesse guastare, lei ha l'obbligo di informare immediatamente _____.

Allegato 5. Modello lettera istruzioni soggetto autorizzato (visualizzazione e registrazione)

MODELLO DI ISTRUZIONI DA INTEGRARE IN LETTERA DI AUTORIZZAZIONE SU FAC SIMILE UNIVERSITA' A SECONDA DELL'IMPIANTO E DEL PROFILO DI AUTORIZZAZIONE.

In caso di nomina a Responsabile del Trattamento, il fornitore è tenuto a dare istruzioni ai propri soggetti autorizzati secondo il seguente modello.

Il trattamento di immagini avviene secondo normativa applicabile di legge.
Lei verificherà che il trattamento delle immagini rilevate dai sistemi di videosorveglianza vengano trattate nel rispetto della protezione dei dati personali, e in particolare:

- che in ogni circostanza le azioni eseguite che comportano trattamento dei dati personali devono essere limitate a quanto strettamente necessario in relazione al perseguimento delle finalità dell'impianto e con i limiti qui indicati;
- che sia rispettato l'obbligo di massima riservatezza in relazione a qualsiasi informazione o dato personale acquisito;
- la password di accesso al monitor è personale, riservata e non cedibile;
- le persone non autorizzate alla visione delle immagini non possono accedere al locale in cui sono collocati i monitor. A tale scopo andrà affisso apposito cartello recante il divieto sulla porta del locale; tale divieto dovrà essere fatto valere nei confronti di chiunque;
- i monitor devono essere orientati in modo da escludere la visione anche accidentale delle immagini a persone non autorizzate che si trovino all'esterno del locale;
- il locale in cui sono collocati i monitor non può essere mai lasciato incustodito; in caso di allontanamento la porta di accesso deve essere chiusa a chiave;
- le operazioni diverse dalla visione sulle immagini, quali la copia, la modifica, la cancellazione, la comunicazione, la divulgazione o altro trattamento delle immagini con qualsiasi mezzo, sono vietate;
- la comunicazione dei dati personali acquisiti attraverso la visione delle immagini è consentita esclusivamente al referente interno;
- la diffusione dei dati personali acquisiti attraverso la visione delle immagini è vietata senza eccezioni;
- i monitor devono essere spenti dall'utente alla cessazione del proprio turno di servizio.

Lei è autorizzato alla visione in tempo reale delle immagini risultati dai monitor presenti in _____, oltre all'accesso alle registrazioni alle condizioni di seguito indicate.
L'accesso alle registrazioni è consentito solo in caso di rilevazione o sospetto di atti illeciti o per effettuare verifiche sulla funzionalità dei sistemi o su richiesta dell'Autorità giudiziaria.
In caso di rilevazione o sospetto di atti illeciti o per effettuare verifiche sulla funzionalità dei sistemi, lei dovrà accedere utilizzando le sue credenziali d'accesso personali riservate fornite, informando _____. Qualora a tale operazione assista personale di manutenzione, anche di soggetti esterni, Lei non dovrà allontanarsi senza aver prima disabilitato l'accesso alle immagini registrate.
In caso di richieste di accesso alle immagini registrate, lei dovrà accedere utilizzando le sue credenziali d'accesso fornite personali riservate, previa autorizzazione da parte di_____.