UNIVERSITÀ DEGLI STUDI DI TRIESTE

Area Contratti e Affari generali
Settore Servizi amministrativi generali
Ufficio Affari generali e Trasparenza amministrativa

Oggetto: Emanazione del Regolamento sul trattamento dei dati personali tramite impianto di videosorveglianza

IL RETTORE

Vista la Legge 20 maggio 1970, n. 300 recante lo Statuto dei lavoratori;

Vista il Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e successive modifiche;

Visto il provvedimento del Garante per la protezione dei dati personali in materia di videosorveglianza dell'8 aprile 2010;

Visto il Regolamento generale per la protezione dei dati personali (GDPR) n. 679/2016;

Vista la Circolare dell'Ispettorato Nazionale del Lavoro del 19 febbraio 2018, n. 5, sull'installazione e utilizzazione di impianti audiovisivi e altri strumenti di controllo ai sensi dell'art. 4 dello Statuto dei lavoratori

Richiamato il "Regolamento in materia di protezione dei dati personali dell'Università degli Studi di Trieste", emanato con il decreto rettorale n. 512 dell'8 agosto 2019;

Viste le linee guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate dal Comitato europeo per la protezione dei dati il 29 gennaio 2020;

Preso atto che nel mese di febbraio 2023 è stata raggiunta l'intesa con le rappresentanze sindacali d'Ateneo in merito alla stipula dell'Accordo integrativo sull'impiego dei sistemi di videosorveglianza presso le strutture, aree di pertinenza e sedi dell'Università degli Studi di Trieste;

Ritenuto necessario un apposito regolamento per disciplinare l'utilizzo dei sistemi di videosorveglianza;

Richiamata la deliberazione del Consiglio di Amministrazione del 3 marzo 2023 che ha approvato il Regolamento sul trattamento dei dati personali tramite impianto di videosorveglianza.

DECRETA

art. 1 – di emanare il Regolamento sul trattamento dei dati personali tramite impianto di videosorveglianza, nel testo posto in allegato.

art. 2 – di stabilire che il Regolamento sul trattamento dei dati personali tramite impianto di videosorveglianza, per ragioni di urgenza, entri in vigore il giorno successivo alla pubblicazione nell'Albo Ufficiale di Ateneo del presente provvedimento.

art. 3 – di incaricare l'Area dei Servizi tecnici e di supporto e l'Ufficio Affari generali e Trasparenza amministrativa, per le parti di rispettiva competenza, dell'esecuzione

Università degli Studi di Trieste
Piazzale Europa, 1
I - 34127 Trieste
www.units.it – ateneo@pec.units.it

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

del presente provvedimento, che verrà registrato nel repertorio dei decreti del Rettore.

Il Rettore
F.to Prof. Roberto Di Lenarda

Firmato digitalmente da: Roberto Di Lenarda
Organizzazione: UNIVERSITA' DEGLI STUDI DI TRIESTE/80013890324
Unità organizzativa: AREA SERVIZI ICT
Data: 22/03/2023 12:48:54

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

UNIVERSITÀ DEGLI STUDI DI TRIESTE
Area Contratti e Affari generali
Settore Servizi amministrativi generali
Ufficio Affari generali e Trasparenza amministrativa

ALLEGATO

REGOLAMENTO SUL TRATTAMENTO DEI DATI PERSONALI TRAMITE IMPIANTO DI VIDEOSORVEGLIANZA

ART. 1 - OGGETTO ED AMBITO DI APPLICAZIONE

1. Il presente Regolamento, in attuazione dell'art. 32 del Regolamento in materia di protezione dei dati personali dell'Università approvato con Decreto Rettorale n. 514 di data 8/8/2019, disciplina l'utilizzo dei sistemi di videosorveglianza attivati presso le strutture, aree di pertinenza e sedi dell'Università ed il trattamento dei dati personali acquisiti attraverso i medesimi sistemi, in conformità alle disposizioni del GDPR, del Codice, dello Statuto dei lavoratori, delle Linee Guida, nonché agli inerenti provvedimenti ed atti interpretativi e di indirizzo.
2. Le modalità operative per la progettazione, installazione, manutenzione e gestione degli impianti di videosorveglianza sono definite nel manuale operativo pubblicato sul portale gdpr.unityfvg.it e periodicamente aggiornato secondo l'evoluzione dei sistemi e della normativa.
3. Sono chiamati ad applicare e rispettare il presente regolamento il Titolare, i responsabili interni di cui all'art. 12 del citato Regolamento in materia di protezione dei dati personali dell'Università unitamente ai referenti e autorizzati al trattamento da questi designati, l'Area dei Servizi Tecnici e di Supporto per gli ambiti di competenza e gli eventuali responsabili esterni del trattamento o i contitolari, come dettagliato nell'art. 4. Il Responsabile per la protezione dei dati rilascia, quando richiesto, i pareri di competenza.

ART. 2 – PRINCIPI GENERALI E FINALITÀ

1. 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, con particolare riferimento alla riservatezza e all'identità personale, e nel pieno rispetto dei principi di liceità, necessità, proporzionalità, che implicano la limitazione delle finalità e la minimizzazione dei dati, di trasparenza e di partecipazione di cui all'articolo 5 del GDPR.
2. L'installazione e utilizzo dell'impianto richiede una preliminare verifica della base giuridica applicabile di cui all'art. 6 GDPR. In particolare, tale verifica preliminare dovrebbe essere basata su dati oggettivi, parametri e statistiche documentabili in relazione alle specifiche finalità perseguite, al fine di dimostrarne l'attualità e necessità.
3. La progettazione degli impianti e la loro installazione devono rispettare i principi di privacy by design e privacy by default di cui all'art. 25 del GDPR.

4. La progettazione dell'impianto deve inoltre realizzare in modo pertinente la finalità del trattamento nel rispetto della base giuridica e dei principi suindicati, progettando misure tecniche e organizzative pertinenti (a titolo esemplificativo con riferimento alla dimensione, capacità tecniche, limitazioni nel tempo e nello spazio degli impianti, trattamento e stoccaggio dei dati mediante opportuni parametraggi del sistema, definizione di protocolli di gestione delle singole autorizzazioni di accesso e trattamento delle immagini, contratti con i fornitori).
5. L'Università si avvale di sistemi di videosorveglianza esclusivamente per il perseguimento di finalità di interesse pubblico o connesso all'esercizio di pubblici poteri e, in particolare, delle seguenti finalità:
    a. 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;
    b. tutelare il patrimonio mobiliare e immobiliare, di proprietà o in gestione dell'Università, da atti vandalici, furti e danneggiamenti;
    c. cooperare alla tutela dell'ordine e della sicurezza pubblica ed alla rilevazione, alla prevenzione e all'accertamento di illeciti;
    d. beneficiare dell'azione deterrente, insita nei sistemi di sorveglianza.
6. L'utilizzo degli impianti di videosorveglianza è effettuato laddove necessario e non sia stato possibile individuare misure alternative meno invasive dei diritti e libertà degli interessati. La verifica della necessità è basata su dati oggettivi, parametri e statistiche documentabili in relazione alle specifiche finalità perseguite, al fine di dimostrarne l'attualità e necessità.
7. È vietata l'installazione di telecamere finte o non funzionanti, nascoste o occulte.

ART. 3 - TUTELA DEI LAVORATORI

1. I sistemi di videosorveglianza non possono essere utilizzati per effettuare controlli a distanza sull'attività lavorativa del personale dell'Università e di tutti coloro che operano a vario titolo nell'Università, in conformità a quanto previsto dallo Statuto dei lavoratori e dal CCNL in vigore del pertinente Comparto.
2. Laddove dai sistemi installati per le finalità sopra elencate (art. 2) 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 specifico e ulteriore accordo collettivo con le Organizzazioni sindacali/RSU di Ateneo ovvero, in mancanza di accordo, previa autorizzazione della 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.
3. Resta in ogni caso esclusa la possibilità di ripresa negli uffici/locali dove il personale universitario presta la propria attività lavorativa.
4. Il soggetto incaricato ad applicare le procedure necessarie per la stipula di accordi sindacali ai sensi dell'art. 4, L. 300/1970 è di seguito indicato:

Azione	**Funzione responsabile**
Redazione accordo	Competente Ufficio della Direzione Generale
Approvazione	Consiglio di Amministrazione

ART. 4 – FUNZIONI E RESPONSABILITA'

1. I soggetti chiamati ad applicare il presente regolamento sono i seguenti:

Legale rappresentante – Rettore
DPO (Responsabile per la protezione dei dati)
Area dei Servizi Tecnici e di Supporto
Gruppo di supporto al Responsabile per la Protezione dei Dati
Soggetti autorizzati al trattamento dei dati personali
Responsabili esterni del trattamento
Contitolari del trattamento

ART. 5 - 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.
2. 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 del GDPR.
3. 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.

ART. 6 – INSTALLAZIONE E DISLOCAZIONE DEI SISTEMI DI VIDEOSORVEGLIANZA

1. L'individuazione dei sistemi di videosorveglianza dell'Università è descritta in appositi documenti custoditi dall'Area dei Servizi Tecnici e di Supporto secondo le procedure individuate nel manuale operativo.
2. Nei menzionati 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.
3. 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 dei Servizi Tecnici e di Supporto è individuato quale soggetto designato ai sensi dell'art. 2 quater decies del Codice ai fini dell'applicazione del presente regolamento con i compiti e secondo le procedure individuati nel manuale operativo.

ART. 7 - CONSERVAZIONE DEI DATI

1. Le immagini registrate vengono conservate per il periodo strettamente necessario e proporzionale al perseguimento delle finalità indicate agli interessati e comunque non superiore a 7 giorni dalla loro rilevazione, decorso il quale devono essere automaticamente cancellate, in conformità a quanto previsto dal successivo art. 9.
2. Rimangono salve speciali esigenze di ulteriore conservazione connesse a festività o periodi di chiusura delle sedi dell'Università, ovvero a specifiche richieste di autorità giudiziaria o polizia giudiziaria, per finalità di prevenzione, accertamento o repressione di reati.

ART. 8 - CANCELLAZIONE DEI DATI

1. Decorso il termine di conservazione dei dati di cui al precedente art. 7, le immagini registrate devono essere automaticamente cancellate dai relativi supporti, secondo le modalità più efficaci individuate dall'Area dei Servizi Tecnici e di Supporto, in modo tale da rendere inutilizzabili i dati cancellati.

ART. 9 - DIVIETO DI COMUNICAZIONE E DIFFUSIONE DEI DATI

1. Sono vietate la comunicazione e la diffusione delle immagini registrate a soggetti non autorizzati.

2. 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.
3. In caso di raccolta di immagini di fatti concernenti ipotesi di reato, segnalate dalle Autorità competenti, o di eventi rilevanti ai fini della pubblica sicurezza o dell'ordine pubblico, l'Università è tenuta a darne tempestiva comunicazione all'autorità giudiziaria.

ART. 10 - TITOLARE DEL TRATTAMENTO

1. Titolare del trattamento dei dati personali raccolti con i sistemi di videosorveglianza è l'Università.

ART. 11. - 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. Qualora l'installazione, gestione o manutenzione dell'impianto comporti la comunicazione di dati personali a soggetti terzi in qualità di responsabili del trattamento ai sensi dell'art. 28 GDPR, i contratti stipulati devono includere i requisiti previsti dal presente Regolamento e dal manuale operativo, al fine di garantire il rispetto dello stesso livello di protezione dei dati personali durante il loro intero ciclo di vita.
3. Le medesime disposizioni si applicano nei confronti di eventuali contitolari del trattamento.

ART. 12 - AUTORIZZATI AL TRATTAMENTO

1. Il Titolare, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, assegna compiti e funzioni connessi alle attività di videosorveglianza a soggetti che operano sotto la propria autorità, debitamente istruiti su tali trattamenti, ai sensi degli artt. 32 del GDPR e 2-quaterdecies del Codice.
2. Gli autorizzati al trattamento curano la manutenzione ordinaria e straordinaria degli impianti di videosorveglianza e la gestione e cancellazione di immagini e dati personali acquisiti attraverso i medesimi, attenendosi alle istruzioni operative impartite dal Titolare o da soggetti esterni eventualmente nominati da quest'ultimo quali Responsabili del trattamento (art. 11 del Regolamento).

ART. 13 – INFORMATIVA

1. L'Università informa gli interessati in ordine alla presenza negli spazi della stessa di sistemi di videosorveglianza mediante l'affissione nelle zone interessate, in prossimità della

videocamera, di un'informativa cosiddetta "minima" (cartello), secondo il modello indicato nelle Linee guida e personalizzato secondo le indicazioni contenute nel manuale operativo.

2. L'informativa è collocata prima del raggio di azione della videocamera e deve avere 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, un'informativa estesa, contenente tutti gli elementi di cui agli articoli 13 e 14 del GDPR.

ART. 14 - DIRITTI DELL'INTERESSATO

1. L'Università garantisce a ciascun soggetto, i cui dati personali siano stati acquisiti mediante i sistemi di videosorveglianza di sé medesima, l'esercizio dei propri diritti, in conformità a quanto disposto dagli articoli 15 e ss. del GDPR.
2. Sono, in particolare, garantiti il diritto di accedere ai propri dati, al solo fine di verificare le modalità di trattamento, e il diritto di ottenere la cancellazione o la limitazione dei dati trattati in violazione di legge ovvero il diritto di opposizione.
3. L'interessato esercita i propri diritti presentando apposita istanza scritta all'Università, secondo le modalità indicate nell'informativa in forma estesa di cui al precedente art. 13.

ART. 15 - NORMA DI RINVIO

1. Per tutti gli aspetti non espressamente disciplinati dal presente regolamento si rinvia alle normative vigenti ed ai provvedimenti e atti interpretativi e di indirizzo in materia di trattamento dei dati personali e di videosorveglianza.

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Area Contratti e Affari generali
Settore Servizi amministrativi generali
Ufficio Affari generali e Trasparenza amministrativa

TRATTAMENTO DEI DATI PERSONALI TRAMITE IMPIANTO DI VIDEOSORVEGLIANZA

- MANUALE OPERATIVO -

Università degli Studi di Trieste

INDICE

Università degli Studi di Trieste
Piazzale Europa, 1
I - 34127 Trieste
www.units.it – ateneo@pec.units.it

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

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 trat-	XXXX

tamento ex art. 28 GDPR	
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.

UNIVERSITÀ DEGLI STUDI DI TRIESTE

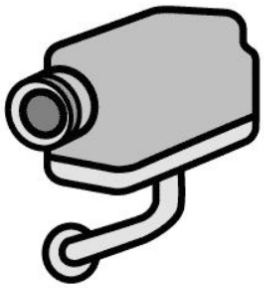
Area Contratti e Affari generali
Settore Servizi amministrativi generali
Ufficio Affari generali e Trasparenza amministrativa

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



AREA VIDEOSORVEGLIATA

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

DIRITTI DEGLI INTERESSATI:

Come soggetto interessato puoi esercitare i tuoi diritti, in particolare il diritto di chiedo

Università degli Studi di Trieste
Piazzale Europa, 1
I - 34127 Trieste
www.units.it – ateneo@pec.units.it

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

dell'art. 13 GDPR sul trattamento dei dati personali accedere al seguente indirizzo: **inserire link** o consultare il testo affisso presso XXX/URP.	re 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.

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Area Contratti e Affari generali
Settore Servizi amministrativi generali
Ufficio Affari generali e Trasparenza amministrativa

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.

Università degli Studi di Trieste
Piazzale Europa, 1
I - 34127 Trieste
www.units.it – ateneo@pec.units.it

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

UNIVERSITÀ DEGLI STUDI DI TRIESTE
Area Contratti e Affari generali
Settore Servizi amministrativi generali
Ufficio Affari generali e Trasparenza amministrativa

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?	

Università degli Studi di Trieste
Piazzale Europa, 1
I - 34127 Trieste
www.units.it – ateneo@pec.units.it

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

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?	

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

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?	

UNIVERSITÀ DEGLI STUDI DI TRIESTE
Area Contratti e Affari generali
Settore Servizi amministrativi generali
Ufficio Affari generali e Trasparenza amministrativa

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 mobi-

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

	liare 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 riva-

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

lutati 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

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Area Contratti e Affari generali
Settore Servizi amministrativi generali
Ufficio Affari generali e Trasparenza amministrativa

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_____.

Responsabile del procedimento: dott.ssa Serena Bussani
Tel. +39 040 558 3017 - 7878
aaggdocc@amm.units.it