



Coordinamento Privacy

**AZIENDA OSPEDALIERA UNIVERSITARIA
FEDERICO II**

Regolamento Privacy Videosorveglianza

A cura
dell'ufficio privacy

Il responsabile della Protezione dei Dati
Ing. Guglielmo Toscano

Storia del documento

Data	Versione	Descrizione modifiche	Autore
25/10/2023	1.0	Prima stesura	Ing. Guglielmo Toscano, Avv. Alessandra Migliaccio
15/06/2024	1.1	Seconda stesura	Ing. Guglielmo Toscano, Dott. Gianpiero Uricchio

Sommario

PREMESSA	4
ART.1 DEFINIZIONI	5
ART.2 PRINCIPI GENERALI.....	5
ART.3 NORMATIVA DI RIFERIMENTO	7
ART. 4 SCOPO.....	7
ART. 5 APPLICABILITA'	7
ART.6 TUTELA DEI LAVORATORI	8
ART.7 COMPOSIZIONE DELL'IMPIANTO.....	8
ART.8 TIPOLOGIA E MODALITÀ DI RIPRESA	8
ART.9 SOGGETTI.....	9
ART. 10 MISURE DI SICUREZZA	9
ART.11 TITOLARE, RESPONSABILI ED INCARICATI DEL TRATTAMENTO DEI DATI.....	10
ART.12 CONSERVAZION DEI DATI.....	11
ART.13 INSTALLAZIONE DI IMPIANTI DI VIDEOSORVEGLIANZA	11
ART.14 MISURE DI SICUREZZA	12
ART.15 INFORMATIVA	12
ART.16 SANZIONI E AZIONI DI RIPRISTINO.	13
ART.17 DPIA (Data Protection Impact Assessment)	14
ART. 18 DISPOSIZIONI FINALI.....	14

PREMESSA

L'A.O.U. Azienda Ospedaliera Universitaria Federico II, nel pieno rispetto dei diritti e delle libertà fondamentali dei cittadini, della dignità delle persone, con particolare riferimento alla riservatezza, all'identità e alla protezione dei dati personali, adotta il presente regolamento aziendale in materia di utilizzo di impianti di videosorveglianza.

L'attività di videosorveglianza avviene in conformità delle norme legali e contrattuali vigenti, nel rispetto del principio di tutela della dignità e riservatezza dei lavoratori, nonché del principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione e nel rispetto del principio di pertinenza, e di non eccedenza relativamente alla raccolta dei dati, in attuazione e nei limiti di quanto stabilito dalle norme europee e italiane in materia di privacy (precisamente dal GDPR 2016/679, dal Codice privacy 196/2003 così come novellato dal decreto legislativo 101/2018, nonché dal Provvedimento Generale sulla videosorveglianza emanato dal Garante Privacy in data 08.04.2010).

Il Comitato Europeo per la Protezione dei Dati, consapevole dell'invasività nella sfera personale di un sistema di videosorveglianza e/o videocontrollo, ha adottato, in data 29 gennaio 2020, le linee guida n. 3/2019, il primo documento europeo che applica i principi del GDPR al trattamento dei dati personali tramite riprese video.

Inoltre, con riferimento all'art. 3.1 del "Provvedimento generale sulla videosorveglianza" e di quanto suggerito dalle Linee guida EDPB ai punti 7.1 e seguenti che prevedono:

- a) Una informativa di primo livello agli interessati che devono essere informati dell'accesso o del transito in una zona videosorvegliata e dell'eventuale registrazione, come da modello semplificato di informativa "minima" individuato dal Garante, da attuarsi mediante cartelli segnalatori;
- b) Un'informativa di secondo livello con avviso circostanziato, che riporti gli elementi dell'art.13 del Regolamento UE 2016/679, con particolare riferimento alle finalità individuate e all'eventuale conservazione dei dati raccolti;

Il presente regolamento aziendale è predisposto tenendo conto anche delle indicazioni fornite dall'Autorità Garante, per la Protezione dei Dati Personali con il provvedimento dell'8 aprile 2010, in base alle quali le ragioni delle scelte organizzative del Titolare devono essere adeguatamente documentate in un atto conservato presso il Titolare stesso e il Responsabile del trattamento, e ciò anche fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso dinanzi all'autorità giudiziaria.

ART.1 DEFINIZIONI

Ai fini del presente regolamento si intende per

- a) **“videosorveglianza”**, il sistema o il dispositivo elettronico volto a riprendere delle immagini, aree, o zone delimitate;
- b) **“trattamento”** qualunque operazione o complesso di operazioni, concernenti la raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, selezione, estrazione, utilizzo dei dati;
- c) **“dato personale”**, qualunque informazione relative a persona fisica identificata, o identificabile, mediante riferimento a qualsiasi informazione; l’immagine di una persona ripresa tramite I sistemi di videosorveglianza equivale a dato personale;
- d) **“Interessato”**, la persona fisica cui si riferiscono i dati;
- e) **“diffusione”** il dare conoscenza dei dati mediante la messa a disposizione o consultazione;
- f) **“informativa”** informa li interessati che stanno per accedere in una zona videosorvegliata ai sensi dell’art. 13 del Codice Privacy.

ART.2 PRINCIPI GENERALI

La videosorveglianza è finalizzata allo svolgimento delle funzioni istituzionali della A.O.U Azienda Ospedaliera Universitaria Federico II, tenuto conto delle esigenze derivanti dalla organizzazione aziendale.

Il trattamento dei dati personali attraverso il sistema di videosorveglianza è effettuato in ottemperanza ai principi di liceità, proporzionalità, finalità, e necessità per garantire la sicurezza, l’efficacia e la protezione di beni, e persone; I principi sono come di seguito definiti:

1. **Principio di liceità**: il trattamento dei dati personali, effettuato attraverso i sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali ovvero:
 - a) Per il perseguimento di finalità di sicurezza sanitaria, gestione dei servizi I assistenza sanitaria, garantire maggiore sicurezza ai pazienti ed operatori;
 - b) Per il controllo sulla sicurezza degli ambienti di lavoro, dei pazienti, dei visitatori, dipendenti, ed altri operatori;
 - c) Come misura complementare ai fini della tutela del patrimonio aziendale, del miglioramento della sicurezza all’interno, e all’esterno delle single strutture, prevenendo atti di danneggiamento.

Il Titolare basa il trattamento in oggetto sulle seguenti condizioni di liceità ex art 6 e 9 del GDPR:

- a) Legittimo interesse (art 6, p.1, let. f, GDPR), reale ed attuale;
- b) Esecuzione di un compito di interesse comune (art 6, lett. e, GDPR);
- c) sicurezza sociale e protezione sociale, (art. 9, p. 2, considerando 52, GDPR).

La videosorveglianza e/o il videocontrollo avvengono nel rispetto oltre che nella disciplina in materia di protezione dei dati personali, di tutela della dignità dell'immagine, del domicilio e degli altri luoghi, cui è riconosciuta analoga tutela.

L'Azienda effettua il trattamento di dati attraverso sistemi di videosorveglianza e/o videocontrollo tenendo presenti le norme riguardanti la tutela dei lavoratori ai sensi della legge n. 300 del 1970, "Statuto di Lavoratori".

2. Principio di proporzionalità

L'installazione degli impianti di videosorveglianza sono proporzionati all'effettivo grado di rischio presente nell'area, e possono essere attivati quando altre misure (il controllo da parte di addetti, sistemi di allarme, misure di protezione agli ingressi, illuminazione adeguata) siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.

3. Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi, è consentita la videosorveglianza come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

4. Principio di necessità

Gli scopi finalizzati, devono essere legittimi, espliciti, e determinati, secondo il GDPR.

Il Titolare del trattamento comunica nell'informativa le finalità perseguite dall'installazione di impianti di videosorveglianza e controllo.

L'informativa deve essere chiaramente conoscibile e visibile da parte degli interessati.

ART.3 NORMATIVA DI RIFERIMENTO

- D.lgs. n. 101/2018

Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR).

- D.lgs. n. 196/2003

Decreto Legislativo n. 196 del 30 giugno 2003, contenente il “Codice in materia di protezione dei dati personali”, n. c. “Codice Privacy”.

-Regolamento UE 2016/679

Regolamento 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).

-Legge n. 300/1970

Statuto dei Lavoratori.

-Linee guida EDPB 3/2019

Linee guida in materia di videosorveglianza secondo il regolamento (UE) 2016/679, rilasciate dall'EDPB il 29 gennaio 2020.

-D.lgs. 9 aprile 2008 n.81 Testo Unico sulla salute e sicurezza sul lavoro.

ART. 4 SCOPO

Il documento ha lo scopo di:

- Analizzare analiticamente tutte le fasi di gestione operative di eventuali problemi connessi alle operazioni di videosorveglianza effettuate dal Titolare;
- definire la procedura operativa generale di gestione della videosorveglianza adottata dalla **AOU Azienda Ospedaliera Universitaria Federico II;**

L'ente con il progetto di videosorveglianza vuole potenziare gli strumenti in suo possesso per il controllo e la sorveglianza, per ragioni di sicurezza. La videosorveglianza è uno strumento di prevenzione e di razionalizzazione dell'azione e degli interventi di chi è preposto a tutelare le esigenze di sicurezza.

ART. 5 APPLICABILITA'

Il presente Regolamento si applica a tutti gli impianti di videosorveglianza e di videocontrollo

installati sia all'interno che all'esterno delle strutture dell'Ospedale nel rispetto dei principi, le regole e le prescrizioni adottate al fine di dare attuazione al presente Regolamento aziendale sulla videosorveglianza in conformità alle disposizioni dettate a tutela dei dati personali dal Regolamento UE 2016/679, dai provvedimenti del Garante per la protezione dei dati personali, oltre che dalle vigenti norme dettate dallo Statuto dei lavoratori e in tema di sicurezza sul lavoro.

ART.6 TUTELA DEI LAVORATORI

L'uso di impianti di videosorveglianza, vietato per finalità di controllo a distanza dei lavoratori, è ammesso per le finalità di:

- protezione delle persone, all'interno ed all'esterno delle singole strutture aziendali, ed a prevenzione dei reati;
- sicurezza degli ambienti di lavoro;
- Tutela dei beni, ed in particolare prevenzione dei reati contro il patrimonio dell'azienda, dei dipendenti, e degli utenti;

Le immagini registrate possono essere messe a disposizione dell'Autorità Giudiziaria e di Pubblica Sicurezza con le modalità previste dalla legge.

ART.7 COMPOSIZIONE DELL'IMPIANTO

L'impianto di videosorveglianza e videocontrollo in uso presso l'Azienda, essendo la stessa articolata nel presidio ospedaliero, è prevalentemente strutturato nel sistema composto da più telecamere, da un'unità di commutazione e smistamento delle immagini, da una centrale di controllo, e da un'unità di registrazione (NVR). La specifica analitica dell'impianto, unitamente all'indicazione della localizzazione delle telecamere e della modalità di ripresa – in aderenza alle finalità che hanno suggerito l'installazione del sistema di videosorveglianza, specialmente in ordine ai principi di pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti – sono presenti nell'allegato Caratteristiche Tecniche dell'impianto e conservate agli atti dell'U.O.C. Tecnico Patrimoniale.

ART.8 TIPOLOGIA E MODALITÀ DI RIPRESA

Tutti gli impianti di videosorveglianza installati in Azienda (sia all'interno della struttura che negli spazi adiacenti) effettuano la registrazione delle immagini. Le telecamere devono essere installate e posizionate in modo da raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando (quando non indispensabile) immagini dettagliate o dettagli comunque non rilevanti.

La localizzazione delle telecamere e le modalità di ripresa sono determinate in ottemperanza a quanto sopra precisato. L'angolatura e la panoramica delle riprese devono essere effettuate con modalità tali da limitare l'angolo di visuale all'area per il controllo della quale si installa il sistema di videosorveglianza, evitando di inquadrare zone private non interessate alla finalità dell'impianto.

Si precisa che le telecamere sono in modalità registrazione, non accessibili a nessuno se non dietro specifica richiesta da parte dell'autorità giudiziaria. Solo alcune telecamere, per ragioni di sicurezza, saranno visionabili tramite monitor da soggetti appositamente autorizzati.

I monitor degli impianti di videosorveglianza devono essere collocati preferibilmente in locali appartati, ove non vi sia afflusso di persone estranee all'Azienda. In ogni modo la collocazione dei monitor deve essere tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee.

ART.9 SOGGETTI

Le Direzioni Mediche Generali dell'Azienda anche su richiesta dei Direttori/Responsabili delle UU.OO.CC / UU.OO.SS.DD aziendali, in quanto delegate interne al trattamento dei dati, valutano la necessità dell'installazione di eventuali impianti di videosorveglianza / videoregistrazione nel rispetto dei principi di minimizzazione e proporzionalità, in relazione alla finalità da perseguire.

Valutata la necessità concreta di installazione di un impianto di videosorveglianza, le Direzioni Mediche Generali, inoltrano la richiesta, motivata e relazionata, al Titolare che si riserverà di effettuare una ulteriore valutazione, all'U.O.C Tecnico Patrimoniale ed all'U.O.C Privacy.

ART. 10 MISURE DI SICUREZZA

L'accesso ai locali ove sono ubicati i sistemi di visualizzazione è di norma consentito solamente al Titolare o a persone da questi delegate e agli incaricati di cui ai successivi paragrafi, nonché ai tecnici addetti all'assistenza e alla manutenzione degli impianti. I soggetti abilitati ad accedere al sistema di videosorveglianza sono tenuti ad osservare scrupolosamente il presente Regolamento, con particolare riferimento alla corretta acquisizione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato realizzato l'impianto.

I supporti contenenti le immagini soggette a conservazione devono essere riposti in luoghi sicuri.

La cancellazione delle immagini dovrà avvenire preferibilmente mediante il riutilizzo del supporto; ad ogni modo le operazioni di cancellazione dovranno essere effettuate solo ed esclusivamente sul luogo di lavoro. Nel caso in cui il supporto debba essere sostituito per eccessiva usura questo dovrà essere distrutto in modo da renderlo inutilizzabile.

I supporti di memorizzazione delle riprese contenenti dati sensibili non devono riportare esternamente l'indicazione di nominativi o comunque di dati atti ad identificare i soggetti ripresi nelle registrazioni.

ART.11 TITOLARE, RESPONSABILI ED INCARICATI DEL TRATTAMENTO DEI DATI

Il Titolare del Trattamento dei dati raccolti con i sistemi di videosorveglianza è l'A.O.U. Azienda Ospedaliera Universitaria Federico II di Napoli, nella persona del suo rappresentante legale pro-tempore. Il Titolare - o persona da lui delegata - provvede con apposito atto ad autorizzare all'accesso alle immagini il personale all'uopo individuato, a norma dell'art. 2- quaterdecies del Codice Privacy. L'autorizzazione degli operatori designati al trattamento deve contenere lo specifico riferimento alle attività di utilizzo e gestione dei sistemi di videosorveglianza, unitamente alle istruzioni sulle operazioni consentite e deve essere formalizzata utilizzando il modello predisposto dall'Azienda. Secondo tale modello gli autorizzati possono essere abilitati alla sola visione delle immagini sui monitor in sincronia con la ripresa o anche alla visione delle immagini già registrate e alla loro duplicazione/cancellazione.

Il numero degli autorizzati addetti alle operazioni duplicazione/cancellazione, rispetto alla sola visione, deve essere limitato. La responsabilità dell'impianto e del trattamento dei dati relativi agli impianti di videocontrollo, qualora installati per la finalità di cura/monitoraggio pazienti, è affidata ai Direttori e ai Coordinatori delle Unità Operative ospedaliere presso cui è installato tale impianto. Tutto il personale medico ed infermieristico della unità operative in cui è ubicato l'impianto di videocontrollo è per sua natura da considerarsi legittimato, e quindi autorizzato alla visione delle immagini sui monitor.

I responsabili sono persone fisiche che esercitano funzioni direttive nei settori organizzativi, in cui risultano installati i sistemi di videosorveglianza.

Il Responsabile dovrà attenersi alle istruzioni impartite dal Titolare, e avrà il compito di:

- Adottare le misure di sicurezza e gli interventi disposti dal Titolare del trattamento;
- Informare prontamente il Titolare di tutte le questioni rilevanti in materia di videosorveglianza e di trattamento dei dati personali;
- vigilare sul trattamento delle immagini e dei dati da parte degli incaricati;
- custodire i monitor e le apparecchiature del sistema di videosorveglianza;
- adottare le misure necessarie affinché l'accesso ai locali e/o archivi della videosorveglianza sia protetto e limitato ai soli soggetti autorizzati;
- accedere alle registrazioni effettuate, nei casi consentiti;

- evitare la comunicazione di dati per scopi diversi da quelli perseguiti con l'installazione dell'impianto, e per finalità diverse da quelle autorizzate;
- controllare il buon funzionamento dell'impianto installato in caso di presentazione di anomalie;
- evitare che alla macchina ove vengono registrate le immagini acceda personale non autorizzato;
- mantenere l'assoluta riservatezza e segretezza delle informazioni;
- segnalare al Titolare o al Responsabile eventuali problemi applicativi rispetto all'attuazione e all'adempimento degli obblighi previsti dal Codice Privacy.

L'azienda, ai sensi del Regolamento UE, in qualità di titolare è responsabile della gestione e del trattamento delle immagini (che non sono archiviate). Egli vigila sull'utilizzo dei sistemi e sul trattamento dei dati e delle immagini in conformità agli scopi perseguiti dall'Ente ed alle altre disposizioni normative che disciplinano la materia ed in particolare alle eventuali disposizioni impartite dall'Autorità Garante per la protezione dei dati personali.

L'azienda designa e nomina gli incaricati a cui affida i compiti specifici e le prescrizioni per l'utilizzo dei sistemi. Alle immagini in diretta provenienti dalle varie videocamere possono accedere soltanto i dipendenti che prestano servizio nella postazione di controllo dell'accesso principale dell'Ente.

Per il dettaglio delle Nomine di Soggetto designato al trattamento e per le Nomine a responsabile del Trattamento si rimanda all'allegato n.2.

ART.12 CONSERVAZION DEI DATI

Nei sistemi che prevedono la registrazione delle immagini, la conservazione delle medesime avverrà nel rispetto del principio di proporzionalità e congruità per un periodo di 72 ore dalla rilevazione, fatte salve esigenze di ulteriore conservazione in considerazione delle particolari esigenze.

Nel caso in cui sussistano comprovate esigenze, il tempo di conservazione delle immagini può essere esteso a 10 giorni successivi alla loro raccolta.

ART.13 INSTALLAZIONE DI IMPIANTI DI VIDEOSORVEGLIANZA

L'installazione degli impianti di videosorveglianza aziendali, oltre ad essere opportunamente motivata, deve essere preceduta da una valutazione tecnica da parte della Direzione Sanitaria, del SIA e del SATM ciascuno per le rispettive competenze, eventualmente con il supporto del DPO; tale valutazione deve tenere conto dei principi generali del GDPR, in particolare del principio di

proporzionalità secondo il quale l'attività di videosorveglianza, è attivata solo nei luoghi in cui altre misure (es. sistemi di allarme, controlli fisici o logistici, misure di protezione agli ingressi) non siano sufficienti, attuabili o parimenti efficaci.

Tale valutazione deve esitare in una relazione contenente la descrizione delle motivazioni per cui si ritiene necessaria l'installazione di un nuovo impianto o la modifica/integrazione di un impianto esistente, nel rispetto dei principi generali e della normativa di settore di cui al presente Regolamento.

Tale relazione, possibilmente corredata di planimetria indicante l'esatta collocazione delle telecamere e il relativo cono di visuale, viene inviata alle rappresentanze sindacali, e al Titolare della protezione dati al fine di valutare se il trattamento sin dalla progettazione risponde ai requisiti richiesti dalla normativa vigente; il Titolare della protezione dati fornirà un parere comprensivo di eventuali prescrizioni e indicazioni in merito alle modalità, accorgimenti e/o procedure particolari da seguire durante l'installazione/modifica/integrazione dell'impianto.

La procedura sopra descritta deve essere seguita anche nel caso di installazione di impianti di videocontrollo con finalità di monitoraggio pazienti.

ART.14 MISURE DI SICUREZZA

I dati trattati con gli impianti di videosorveglianza devono essere protetti da idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato, o non conforme alle finalità di raccolta.

ART.15 INFORMATIVA

Gli interessati devono sempre essere informati del fatto che stanno per accedere in una zona video sorvegliata tramite apposita informativa. A tal fine negli ambienti e negli spazi sottoposti a videosorveglianza l'Azienda installa, in posizione chiaramente visibile, prima del raggio di azione della telecamera, appositi cartelli contenenti l'informativa "minima" e semplificata conforme al modello stabilito dal Garante per la Protezione dei Dati Personali.

L'Azienda mette inoltre a disposizione degli interessati nei siti Intranet e Internet aziendali l'informativa estesa, contenente tutti gli elementi di cui all'art.13 del GDPR.

Tutti coloro che accedono ai locali della A.O.U Federico II, sono opportunamente informati dell'esistenza degli impianti di videosorveglianza nell'area in cui stanno per transitare.

L'obbligo di informativa, come disposto dall'art 13 del Codice Privacy, è adempiuto mediante l'esposizione di cartelli:

– conformi al modello stabilito dal Garante per la protezione dei dati personali

– indicanti la presenza nell’area di una o più telecamere.

L’informativa agli interessati viene inoltre garantita tramite:

- la pubblicazione del presente Regolamento sul sito aziendale all’indirizzo www.policlinico.unina.it nell’apposita sezione Privacy;
- l’apposizione dell’informativa sulla videosorveglianza nelle entrate principali dell’azienda A.O.U Federico II.

Per Maggiori informazioni o dettagli, si veda l’allegato 3 “Informativa estesa Videosorveglianza”.

ART.16 SANZIONI E AZIONI DI RIPRISTINO.

La mancata osservanza delle disposizioni contenute nel presente regolamento, comporta responsabilità disciplinare per coloro che hanno posto in essere il comportamento irregolare, siano essi dipendenti o soggetti assimilati ai dipendenti ai sensi del Codice di comportamento aziendale.

La rilevazione di informazioni ottenute attraverso il sistema di videosorveglianza, oltre a costituire violazione disciplinare, integra la fattispecie del reato di cui all’art 326 del Codice Penale (Rilevazione ed utilizzazione di segreti d’ufficio).

Il trattamento di dati personali effettuato in violazione delle misure minime di sicurezza previste dal Codice privacy, comporta una sanzione amministrativa da diecimila a centoventimila euro;

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento dei dati personali in violazione di quanto disposto dal Codice Privacy è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

In caso di violazione del presente regolamento il Titolare del Trattamento provvederà a porre in atto tutte le azioni necessarie per ripristinare la legalità, disponendo l’immediata interruzione del trattamento in caso di:

- trattamento di dati per scopi non espliciti e non legittimi;
- trattamento di dati in modo non lecito, corretto e pertinente;
- raccolta di dati non pertinenti, non completi ed eccedenti rispetto alle finalità per cui sono stati raccolti.

ART.17 DPIA (Data Protection Impact Assessment)

Ai sensi dell'articolo 35, paragrafo 1, Il Titolare è tenuto ad effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) quando un tipo di trattamento dei dati può comportare un rischio elevato per i diritti e la libertà delle persone fisiche e se il trattamento costituisce un monitoraggio sistematico di un'area accessibile al pubblico su larga scala.

Nello specifico, secondo il chiarimento interpretativo fornito dal Garante per la protezione dei dati personali con l'Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979 - Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018 contenente l' Elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto] la valutazione d'impatto è obbligatoria quando “dai trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).”

Il Titolare del trattamento dei dati dovrebbe quindi effettuare tale valutazione e, sulla base del risultato della DPIA eseguita, dovrebbe determinare la scelta delle misure di protezione dei dati da implementare.

È anche importante notare che se i risultati della DPIA indicano che il trattamento comporta rischi elevati nonostante le misure di sicurezza pianificate dal Titolare del trattamento, sarà necessario prima di iniziare il trattamento consultare l'Autorità di controllo competente.

ART. 18 IMPIANTI SPECIALI

Per tutti i casi specifici relativi a impianti particolari/speciali si rimanda all'allegato n.3.

ART. 19 DISPOSIZIONI FINALI

Per tutto quanto non risulti disciplinato nel presente Regolamento, si rinvia a quanto disposto dal Regolamento UE 2016/679, alle linee guida EDPB 3/2019 ed al provvedimento a carattere generale del Garante per la protezione dei dati personali del 8 aprile 2010.

PROCEDURA PER L'ACCESSO ALLE IMMAGINI

1. La persona interessata ad accedere alle immagini deve avanzare apposita istanza al Titolare del trattamento ovvero al Designato competente e/o al Responsabile della Protezione dei Dati, indicato nell'informativa e nell'apposita sezione del sito web istituzionale.
2. L'istanza deve indicare a quale impianto di videosorveglianza si fa riferimento e le informazioni per risalire al momento esatto della rilevazione. Nel caso le immagini di possibile interesse siano oggetto di conservazione, il richiedente dovrà fornire altresì ulteriori indicazioni, finalizzate a facilitare il reperimento delle immagini stesse, tra cui:
 - il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa;
 - indicazioni sull'abbigliamento indossato, accessori ed altri elementi;
 - presenza di altre persone;
 - attività svolta durante le riprese.

*Nel caso le immagini di possibile interesse non siano oggetto di conservazione, di ciò dovrà essere data formale comunicazione al richiedente.

*Nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data comunicazione al richiedente.
3. Il Titolare del trattamento ovvero il Designato competente accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente;
4. Nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui il suddetto potrà visionare le immagini che lo riguardano.
5. Nel caso il richiedente intenda sporgere reclamo, dovrà presentare apposita istanza, indirizzata al responsabile del trattamento, indicando i motivi del reclamo.
6. Qualora si voglia avere estrazione di copia delle immagini, poiché il titolare ha stabilito un termine congruo entro il quale cancellare le immagini videoregistrate, e poiché altresì l'estrazione di copia è sempre concessa alle Autorità di polizia e Giudiziarie, l'Interessato dovrà richiedere il blocco della cancellazione delle immagini, in attesa di ufficiale richiesta dell'Autorità giudiziaria interpellata

Allegato n.2

NOMINE DESIGNATO AL TRATTAMENTO E NOMINE A RESPONSABILE DEL TRATTAMENTO

Designati al Trattamento (con nomina firmata)

- Dott. Gaetano DORIO

Autorizzati al trattamento

- Operatori interni AOU

Nomine Responsabile del Trattamento

- Società di Vigilanza

IMPIANTI SPECIALI

Impianti localizzati presso gli accessi carrabili e pedonali dell'A.O.U.

- Accesso Via Sergio Pansini n.5
- Accesso Via Tommaso De Amicis
- Accesso Via Santacroce ad Orsolone
- Accesso pedonale Via Gaetano Quagliariello

Impianti nei locali della Farmacia Centralizzata

- Esterni
- Interni

Impianti nei locali del Pronto Soccorso Ostetrico ed. 9.

- Esterni
- Interni

Planimetrie riportante la posizione delle singole Videocamere, inoltre devono essere archiviati le foto dell'inquadratura delle singole Videocamere.