VIDEOSORVEGLIANZA E VIDEOCONTROLLO

Procedura GDPR

Autore: DPO / Supporto Specialistico
Rivisto da U.O.C. Privacy - Trasparenza ed Integrità
Accettato da: DMPO – U.O.C. Tecnico Patrimoniale

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
1	20 / 10 / 2020	Prima versione	DPO
L'ultima revisione sostituisce qualsiasi revisione precedente.			

A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi – Cotugno – CTO

Sommario

PREMESSA

La **A.O.R.N. "Azienda Ospedaliera dei Colli** (d'ora in avanti "Titolare del trattamento" o, più semplicemente, "Titolare"), 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'evoluzione e il progresso tecnologico hanno modificato la fruibilità, la qualità, la velocità della strumentazione di ripresa e di registrazione delle immagini, a fronte di un netto abbassamento dei costi di installazione e di gestione, che ha comportato una notevole diffusione e proliferazione degli impianti di videosorveglianza e videocontrollo.

L'immagine di una persona, sebbene non accompagnata da alcuna didascalia o altra descrizione scritta o sonora, costituisce un dato personale. Per tale motivo, le riprese effettuate per mezzo dei comuni sistemi di videosorveglianza o anche con un semplice videocitofono integrano il trattamento dei dati personali dei soggetti inquadrati dalla telecamera. La presenza di questo sistema di videoripresa deve, quindi, essere opportunamente segnalata con il posizionamento di specifici cartelli di area videosorvegliata.

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 2019, le linee guida n. 3/2019, il primo documento europeo che applica i principi del GDPR al trattamento dei dati personali tramite riprese video.

Il presente regolamento aziendale è predisposto tenendo conto anche delle indicazioni fornite dall'Autorità Garante per la Protezione dei Dati Personali con il provvedimento del dell'8 aprile 2021, 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 ai fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso dinanzi all'autorità giudiziaria.

CAPITOLO 1
AMBITO DI APPLICAZIONE

CAP. 1

❖ SCOPO

Il presente documento ha lo scopo di:

- definire la procedura operativa generale di gestione della videosorveglianza adottata dalla **A.O.R.N. "Azienda Ospedaliera dei Colli**;
- declinare analiticamente tutte le fasi di gestione operativa dei potenziali problemi connessi alle operazioni di videosorveglianza effettuate dal Titolare.

La presente procedura è stata predisposta su proposta e secondo le indicazioni fornite dal Data Protection Officer (DPO) aziendale.

❖ APPLICABILITÀ

La presente procedura è destinata a tutto il personale coinvolto in attività che implicano l'utilizzo di sistemi di videosorveglianza.

❖ SUPPORTO FORNITO DAL DPO

Si specifica che, all'interno della presente procedura, il "supporto" fornito dal DPO della A.O.R.N. Azienda Ospedaliera dei Colli, è di tipo tecnico, attesa la necessaria conoscenza specialistica della normativa e delle prassi in materia di protezione dati, al fine di assolvere i compiti previsti dall'art. 39 del GDPR. Il DPO, infatti, non può in alcun caso prendere decisioni al posto del Titolare del trattamento o sostituirsi nelle valutazioni rimesse dalla normativa data protection in capo a quest'ultimo.

CAPITOLO 2
DEFINIZIONI E NORME DI RIFERIMENTO

CAP. 2

❖ ACRONIMI E ABBREVIAZIONI

DPO	Data Protection Officer – Responsabile della Protezione dei Dati
EDPB	European Data Protection Board – Comitato europeo per la Protezione dei Dati. Organismo europeo indipendente il cui scopo è garantire un'applicazione coerente del GDPR.
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation – Regolamento Generale sulla Protezione dei Dati, n. 2016/679
IT	Information Technology
WP29	Working Group 29: gruppo istituito ai sensi dell'art. 29 della direttiva 95/46 CE. Dal 25 Maggio 2018 prende il nome di European Data Protection Board.

❖ DEFINIZIONI

Archivio	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, n. 6, GDPR).
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica, anche indiretta, dell'identità dell'utente.
Autorità Garante per la Protezione dei Dati Personali	Autorità istituita dalla legge 31 dicembre 1996, n. 675. Ha sede a Roma.
Banca dati	Qualsiasi complesso organizzato di dati (archivio informatico), riguardanti uno stesso argomento o più argomenti correlati tra loro, strutturato in modo tale da consentire la gestione dei dati stessi (l'inserimento, la ricerca, la cancellazione ed il loro aggiornamento) da parte di un'applicazione, ripartito in uno o più elaboratori elettronici (ad es. server, postazioni lavorative, ecc.) dislocati all'interno della rete LAN del Titolare.
Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, c. 1, GDPR).

Centrale di videocontrollo	Sistema che permette la visione, ed eventualmente la registrazione, di tutte le riprese effettuate dai dispositivi periferici.
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento (art. 4, n. 11, GDPR).
Credenziali di autenticazione	I dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, n. 1, GDPR).
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Incaricato del trattamento	Persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile.
Interessato del trattamento	Persona fisica cui si riferiscono i dati personali.
Parola chiave	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti ad una persona fisica identificata o identificabile (art. 4, n. 5, GDPR).
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, n. 8, GDPR).
Sistema di autorizzazione	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
Sistema informativo	L'insieme di dispositivi, programmi ed infrastrutture di rete.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, n. 7, GDPR).

Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, n. 2, GDPR).
Videocitofoni	Sistema o dispositivo installato in corrispondenza di campanelli o citofoni per finalità di controllo dei visitatori che si accingono ad entrare.
Videocontrollo	Sistema o dispositivo che permette la visione unicamente in tempo reale di aree o zone delimitate.
Videosorveglianza	Sistema o dispositivo che permette la visione e la registrazione su supporti singoli, abbinati ad altre fonti o conservati in banche dati di immagini di aree o zone delimitate.
Violazione dei dati personali	Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, n. 12, GDPR).

❖ 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 2019.

CAPITOLO 3
COMPOSIZIONE E GESTIONE DELL'IMPIANTO

CAP. 3

❖ COMPOSIZIONE DELL'IMPIANTO

L'impianto di videosorveglianza e videocontrollo in uso presso l'Azienda, essendo la stessa articolata in tre presidi ospedalieri (Monaldi – Cotugno - CTO), è strutturato in sistemi autonomi ognuno 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) su disco rigido di un personal computer.

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 conservate agli atti dell'U.O.C. Tecnico Patrimoniale.

❖ MODALITÀ DI GESTIONE

Gli impianti di videosorveglianza sono gestiti direttamente dall'AO dei Colli e/o da una o più aziende esterne, in nome e per conto del Titolare del trattamento, il quale ha provveduto a nominarle Responsabili esterni, mediante contratto ex. art. 28 GDPR in cui sono indicati i compiti e le istruzioni cui attenersi.

Il personale autorizzato al trattamento dati mediante sistemi di videosorveglianza e/o videocontrollo sarà designato dal Responsabile esterno o dal Delegato interno della U.O. di riferimento, con lettera nominativa e i nominativi degli stessi saranno riportati su un apposito elenco, tenuto dal Responsabile esterno o dal delegato.

Il Responsabile esterno, unitamente all'atto di nomina, consegnerà ai suoi autorizzati un apposito mansionario contenente le istruzioni di riservatezza e l'obbligo di diligente custodia delle immagini eventualmente estratte. Il Responsabile esterno provvede ad iniziative periodiche di formazione e aggiornamento degli autorizzati, con particolare riferimento ad eventuali modifiche nelle modalità di utilizzo dei sistemi.

Il Responsabile esterno ha l'obbligo di curare la formazione degli autorizzati secondo i principi del GDPR al trattamento dei dati personali tramite riprese video. A prescindere dall'oggetto dell'incarico, è fatto divieto agli autorizzati preposti, la visione e/o estrazione delle immagini registrate, a meno che non ricorrano esigenze di difesa di un diritto, di riscontro ad una istanza di accesso oppure di collaborazione con la competente autorità o polizia giudiziaria.

L'estrazione o la visione delle immagini potrà comunque avvenire solo su richiesta scritta della Direzione Generale o di soggetto, di volta in volta delegato dalla Direzione Generale, oppure su richiesta scritta delle autorità giudiziarie suddette.

CAPITOLO 4
PRINCIPI E FINALITÀ

CAP. 4

❖ PRINCIPIO DI LICEITÀ

Ai sensi del GDPR, l'Azienda effettua il trattamento dei dati attraverso sistemi di videosorveglianza e/o videocontrollo solo ed esclusivamente per lo svolgimento delle proprie funzioni istituzionali, ovvero:

a) per il perseguimento di finalità di sicurezza sanitaria, gestione dei servizi di assistenza sanitaria, monitorare condizioni di salute dei pazienti, garantire maggiore sicurezza ai pazienti e agli operatori;
b) per il controllo sulla sicurezza degli ambienti di lavoro e dei pazienti, visitatori, dipendenti e altri operatori;
c) come misura complementare ai fini della tutela del patrimonio aziendale, del miglioramento della sicurezza all'interno e all'esterno delle singole strutture prevenendo atti di vandalismo o danneggiamento.

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

a) legittimo interesse (art. 6, p. 1, lett. f, GDPR), reale e attuale;
b) esecuzione di un compito di interesse pubblico (art. 6, p. 1, lett. e, GDPR);
c) sicurezza sociale e protezione sociale (art. 9, p. 2 e considerando 52, GDPR).

La videosorveglianza e/o il videocontrollo avvengono nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, di quanto prescritto dalle vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli

altri luoghi cui è riconosciuta analoga tutela e, infine, delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni.

L'Azienda effettua il trattamento dei 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 dei Lavoratori".

❖ PRINCIPIO DI NECESSITÀ

Al trattamento dei dati attraverso sistemi di videosorveglianza e/o videocontrollo è applicato il principio di necessità, come stabilito dal GDPR: qualsiasi trattamento non conforme a questo principio è da ritenersi illecito.

Il sistema a supporto degli impianti di videosorveglianza e/o videocontrollo è conformato in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi.

L'eventuale registrazione di dati personali non necessari deve essere cancellata e i relativi supporti distrutti.

Per l'installazione di sistemi di videosorveglianza che prevedono un intreccio delle immagini con altri particolari sistemi (es. dati biometrici) o in caso di digitalizzazione delle immagini o di sorveglianza che valuti percorsi e lineamenti (es. riconoscimento facciale per accesso a risorse e locali) deve essere effettuata da parte del Titolare una valutazione d'impatto sulla protezione dei dati personali (DPIA), secondo la relativa procedura.

L'installazione delle videocamere nei luoghi di lavoro avviene previo accordo con le R.S.U. aziendali e/o, a seguito dell'autorizzazione della Direzione Provinciale del Lavoro, su istanza del Titolare.

Le videocamere installate, non conformi a questo principio di necessità, seppur non funzionanti dovranno essere rimosse dall'U.O.C. Tecnico Patrimoniale o dal Responsabile esterno, su indicazione del Delegato interno della struttura di riferimento, sentito il Titolare.

❖ PRINCIPIO DI PROPORZIONALITÀ

L'installazione di un sistema di videosorveglianza e/o videocontrollo è proporzionato all'effettivo grado di rischio presente nell'area.

Gli impianti di videosorveglianza e/o videocontrollo possono essere attivati solo quando altre misure (quali il controllo da parte di addetti, sistemi di allarme, misure di protezione degli ingressi e abilitazioni agli ingressi, illuminazione adeguata, vetri antimanomissione, etc.) siano state ritenute insufficienti o inattuabili.

È vietata l'installazione di telecamere non funzionanti anche qualora ciò non comporti trattamento di dati personali.

Va limitata rigorosamente la creazione di banche dati quando è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini senza registrazione.

❖ PRINCIPIO DI FINALITÀ

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

Il Titolare del trattamento comunica nell'informativa le finalità perseguite dall'installazione di impianti di videosorveglianza e/o controllo. L'informativa deve essere chiaramente conoscibile e visibile da parte degli interessati.

CAPITOLO 5
SOGGETTI

❖ DIREZIONI MEDICHE DI PRESIDIO

Le Direzioni Mediche di Presidio, anche su richiesta dei Direttori/Responsabili delle UU.OO.CC. /UU.OO.SS.DD. aziendali, in quanto delegati interni al trattamento dati, valutano la concreta necessità dell'installazione di eventuali impianti di videoregistrazione/videosorveglianza nel rispetto dei principi di minimizzazione e proporzionalità, di cui al punto precedente, in relazione alla finalità da perseguire.
Valutata concreta la necessità di installazione di un impianto di videosorveglianza, le Direzioni Mediche di Presidio inoltrano la richiesta, adeguatamente motivata e relazionata, al Titolare che si riserverà una ulteriore valutazione, all'U.O.C. Tecnico Patrimoniale ed all'U.O.C. Privacy – Trasparenza ed Integrità.

❖ UOC TECNICO PATRIMONIALE

L'U.O.C. Tecnico Patrimoniale, ovvero la struttura interna cui competono le funzioni di progettazione, realizzazione e manutenzione degli impianti installati e da installare, è tenuta ad assicurare la conformità dei suddetti impianti al GDPR, secondo le indicazioni del presente Regolamento e della U.O.C. Privacy – Trasparenza ed Integrità.

❖ DELEGATI INTERNI

I delegati interni ovvero i Direttori/Responsabili delle UU.OO.CC. /UU.OO.SS.DD. aziendali nell'ambito delle quali insistono impianti di videosorveglianza e/o videocontrollo, supportano il Titolare e l'U.O.C. Tecnico Patrimoniale e l' U.O.C. Privacy – Trasparenza ed Integrità ai fini della corretta applicazione del presente regolamento e della normativa di settore alla quale il regolamento si rifà e sono tenuti ad attenersi alle procedure ed istruzioni adottate dal Titolare.

❖ RESPONSABILE ESTERNO

Il soggetto esterno, installatore e/o gestore dell'impianto di videosorveglianza e di videocontrollo, il cui ruolo è formalizzato ai sensi dell'art. 28 del GDPR, deve consegnare al Titolare una descrizione scritta dell'impianto, che ne attesti la conformità alla normativa vigente.
Si rimanda sul punto, anche a quanto indicato nel capitolo 3 del presente regolamento.

❖ AUTORIZZATI AL TRATTAMENTO

Gli autorizzati al trattamento dei dati personali ovvero i soggetti preposti all'utilizzo, alla gestione ed alla manutenzione dei sistemi di videosorveglianza e/o videocontrollo ed alle altre eventuali operazioni di trattamento, vengono nominati dai rispettivi Responsabili esterni o dai delegati interni, con lettera di autorizzazione.

È fatto divieto agli autorizzati di prendere visione delle registrazioni o procedere alla loro estrazione, salvo documentata e motivata richiesta scritta della Direzione Generale o di soggetto, di volta in volta delegato dalla Direzione Generale, oppure su richiesta scritta delle autorità giudiziarie, in relazione a:

a) esercizi di difesa di un diritto;
b) risposta ad una istanza di accesso;
c) richiesta di collaborazione da parte dell'autorità giudiziaria.

CAPITOLO 6
MODALITÀ

❖ RISOLUZIONE ANGOLATURA E PANORAMICA DELLE RIPRESE

La risoluzione delle immagini riprese tramite impianti di videosorveglianza e/o videocontrollo è regolata in modo da riguardare solo i dati strettamente necessari alle finalità perseguite.

Al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (art. 615 bis c.p.), l'angolatura e la panoramica delle riprese deve essere effettuata con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere (spazi di esclusiva pertinenza zonale), evitando aree non necessarie.

❖ INFORMATIVA

Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e/o videocontrollata tramite apposita informativa pubblicata sul sito istituzionale.

Una prima informazione è costituita dalla cartellonistica, che deve essere ben visibile immediatamente prima che l'Interessato possa accedere nell'area videosorvegliata. Qualora la videocamera effettui anche riprese notturne, il cartello deve essere visibile anche di notte.

L'informativa-cartello deve essere collocata nelle immediate vicinanze dei luoghi ripresi, deve avere un formato ed una dimensione che ne permetta un'agevole leggibilità ed un posizionamento tale da essere chiaramente visibile agli interessati.

L'informativa-cartello deve identificare il Titolare del trattamento e specificare le finalità della sorveglianza. Deve, inoltre, menzionare chiaramente se le immagini vengono registrate, fornire informazioni di contatto e il collegamento al sito web aziendale dove acquisire da parte dell'utenza, senza oneri ed agevolmente, il testo completo dell'informativa estesa sulla videosorveglianza.

Qualora siano ancora in circolazione cartelli che fanno riferimento all'art. 13 del d.lgs. 196/2003, abrogato dal d.lgs. 101/2018, è necessario sostituire tali cartelli o correggerli applicando la nuova dicitura: "Reg. EU 2016/679 GDPR e Linee Guida EDPB 3/2019".

❖ TIPOLOGIA DI CARTELLONISTICA UTILIZZABILE

CARTELLI VIDEOSORVEGLIANZA AGGIORNATI		
Cartello videosorveglianza senza registrazione delle immagini	Cartello videosorveglianza con registrazione delle immagini	Cartello videosorveglianza collegata con le forze dell'ordine

		
Testo da inserire: La rilevazione è effettuata da (…) per fini di (…). Le immagini non sono registrate. Per ulteriori informazioni: (sito web). L'accesso alle immagini è consentito esclusivamente al personale autorizzato. Linee Guida EDPB 3/2019 e Reg. EU 2016/679 GDPR.	**Testo da inserire:** La registrazione è effettuata da (…) per fini di (…). Le immagini registrate sono conservate per (…) ore. Per ulteriori informazioni: (sito web). L'accesso alle immagini è consentito esclusivamente al personale autorizzato. Linee Guida EDPB 3/2019 e Reg. EU 2016/679 GDPR.	**Testo da inserire:** La rilevazione è effettuata da (…) per fini di (…). Videosorveglianza collegata con le centrali delle forze dell'ordine. Per ulteriori informazioni: (sito web). L'accesso alle immagini è consentito esclusivamente al personale autorizzato. Linee Guida EDPB 3/2019 e Reg. EU 2016/679 GDPR.

❖ VIDEOSORVEGLIANZA SENZA REGISTRAZIONE – VIDEOCONTROLLO

L'installazione dei sistemi di videocontrollo è vietata nei casi in cui sia sufficiente adottare efficaci dispositivi di controllo alternativi (come la presenza di personale addetto alla vigilanza, etc.), in considerazione del principio di proporzionalità.

La loro presenza, quando necessaria, deve essere segnalata attraverso un'informativa agevolmente rilevabile con le caratteristiche previste da questo regolamento.

L'angolo di visuale e la panoramica delle riprese deve essere effettuata con le modalità previste nel capitolo 6 di questo regolamento.

❖ VIDEOCITOFONI

Ai videocitofoni, solo qualora collegati via web o rete locale, si applicano tutte le regole previste per il videocontrollo.

❖ VIDEOSORVEGLIANZA CON REGISTRAZIONE DELLE IMMAGINI

Si applicano all'installazione dei sistemi di videosorveglianza tutte le regole previste per il videocontrollo (ovvero video sorveglianza senza registrazione).

In applicazione del principio di proporzionalità, la conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario a raggiungere la finalità perseguita (v. Cap. 7).

CAPITOLO 7
MISURE DI SICUREZZA E GESTIONE DEI SUPPORTI

CAP. 7

❖ MISURE DI SICUREZZA

Il trattamento dei dati personali attraverso l'impiego di un sistema di videosorveglianza è equiparato al trattamento dei dati personali a mezzo di strumenti elettronici.
Tra le misure che il Titolare adotta o può adottare per tale trattamento, si segnalano:

- Credenziali di autenticazione distinte per livello di accesso.
  In presenza di differenti competenze specificatamente attribuite ai singoli autorizzati/incaricati, devono essere configurati diversi livelli di accesso e trattamento delle immagini. Se tecnicamente possibile, alla luce delle caratteristiche tecniche degli impianti di videosorveglianza, gli incaricati e i responsabili del trattamento devono disporre di credenziali di autenticazione ad hoc.
- Abilitazione in base alla mansione.
  Se i sistemi di videosorveglianza prevedono la registrazione e la conservazione delle immagini, deve essere limitata la possibilità, per i soggetti abilitati, di prendere visione delle immagini stesse.
- Cancellazione automatica.
  Il sistema deve prevedere la cancellazione in automatico delle immagini registrate, rispettando le scadenze contenute nel presente regolamento.
- Cautele nelle attività di manutenzione.
  L'accesso alle immagini è limitato ai casi ove si renda indispensabile compiere delle verifiche tecniche.
- Protezione da accessi abusivi.
  Nel caso in cui il sistema di ripresa sia collegato a reti telematiche, trova applicazione il disposto di cui all'art. 615 ter c.p.
- Cifratura delle comunicazioni su reti pubbliche.
  La trasmissione tramite reti pubbliche di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata, se prevista, previa applicazione di tecniche di crittografia che garantiscano la riservatezza.

È compito dei soggetti, di cui al Cap. 5, ciascuno per il proprio ambito di competenza, verificare il rispetto delle misure di sicurezza contenute nel presente regolamento e della normativa di settore adottando, o chiedendo l'adozione, di eventuali ed ulteriori misure che si rendano necessarie per evitare il rischio di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.

Della adozione di tali misure di sicurezza sarà fatta menzione nella eventuale DPIA effettuata dal Titolare qualora ritenuta opportuna.

❖ CONSERVAZIONE DELLE IMMAGINI

Stante le finalità degli impianti di videosorveglianza installati in Azienda, valutato in misura "medio" il livello di rischio delle aree sottoposte a controllo, considerate le esigenze di conservazione delle immagini in relazione a festività e/o chiusura delle strutture aziendali, considerata l'esigenza di uniformare sul territorio aziendale la procedura di gestione dei dati trattati mediante videosorveglianza, i dati verranno conservati per un periodo di tempo non eccedente le finalità per le quali sono stati raccolti.

In casi eccezionali, per eventuali esigenze tecniche o per la particolare rischiosità dell'attività svolta, è ammesso un tempo più ampio di conservazione dei dati, che non può comunque superare le 72 ore.

Su specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria, la conservazione delle immagini e le modalità di ripresa potranno subire eccezioni al presente regolamento.

I dati video raccolti per ragioni organizzativo-produttive, per ragioni di sicurezza sul luogo di lavoro o per la tutela del patrimonio aziendale non possono essere utilizzati per finalità diverse (fatte salve eventuali esigenze da parte delle autorità giudiziarie), né possono essere diffusi o comunicati a terzi.

I supporti di memorizzazione delle riprese contenenti categorie particolari di dati personali devono essere opportunamente codificate senza ulteriori indicazioni di nominativi o di date.

Il sistema deve prevedere, in modalità automatica, l'integrale cancellazione delle informazioni allo scadere del termine indicato.

I supporti non più utilizzati devono essere distrutti prima di essere cestinati.

❖ CENTRALI DI VIDEOCONTROLLO E/O VIDEOSORVEGLIANZA – ACCESSO

Le centrali di videocontrollo e/o videosorveglianza sono posizionate in luoghi non facilmente accessibili e comunque controllati; l'accesso è consentito solo al personale autorizzato.

I dispositivi di registrazione sono ulteriormente protetti da serratura o ubicati in luoghi protetti. I supporti di memorizzazione sono conservati in apposito armadio sotto chiave.

La responsabilità di tali adempimenti è dei soggetti, di cui al Cap. 5, ciascuno per il proprio ambito di competenza.

❖ REGISTRO DEI TRATTAMENTI E VALUTAZIONE DI IMPATTO

Il Titolare del trattamento deve costituire apposito registro, o inserire un'apposita sezione per il trattamento dei dati della videosorveglianza nel registro dei trattamenti preesistente, per la disciplina di questo trattamento.

Per tutti i dettagli su tale registro, così come delineato dal GDPR, si rimanda alla procedura specifica conservata in azienda.

La valutazione di impatto (ex. art. 35 GDPR) si configura come un'autonoma valutazione che il Titolare del trattamento pone in essere per analizzare la necessità, la proporzionalità e i rischi di un determinato trattamento dati per i diritti e le libertà delle persone fisiche. La valutazione deve essere effettuata per tutti i trattamenti che possono comportare tale livello di rischio e, in particolar modo per i trattamenti in materia di videosorveglianza, deve essere effettuata secondo il GDPR in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Per determinare se un trattamento è svolto su "larga scala" si deve far riferimento al numero degli interessati, al volume di dati e/o alle tipologie di dati, alla durata dell'attività di trattamento e all'ambito geografico dell'attività di trattamento.

Per tutti i dettagli su come effettuare tale valutazione, così come delineato dal GDPR, si rimanda alle linee guida per la conduzione delle DPIA adottate dall'azienda.

CAPITOLO 8
DISCIPLINA SUI SETTORI SPECIFICI

❖ LUOGHI DI LAVORO

Ai sensi dell'art. 4, l. n. 300/1970, le informazioni raccolte sono utilizzate per tutti i fini connessi al rapporto di lavoro, a condizione che sia data al lavoratore adeguata informazione delle modalità di uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal GDPR.

L'attività di videocontrollo e/o videosorveglianza è ammessa solo ed esclusivamente per finalità di sicurezza negli ambienti di lavoro e di tutela del lavoratore. L'installazione degli impianti deve avvenire previo accordo collettivo stipulato dalla rappresentazione sindacale aziendale. In difetto di accordo, su istanza del datore di lavoro, l'installazione degli impianti deve essere previamente autorizzata dalla Direzione Territoriale del Lavoro.

La ripresa diretta del lavoratore deve essere evitata per quanto possibile.

L'installazione e l'utilizzo degli impianti di videosorveglianza e/o videocontrollo segue quanto previsto dal GDPR e dal capitolo 6 del presente regolamento.

Non è consentito installare apparecchiature di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (quali bagni, spogliatoi, punti di ristoro, in prossimità dei cartellini marcatempo, etc.).

Il mancato rispetto di quanto sopra comporta l'avvio di una verifica e di un procedimento dinanzi all'Autorità Garante della Protezione dei Dati Personali e la possibile applicazione delle sanzioni amministrative stabilite all'interno del GDPR, ove sia stata rilevata l'infrazione.

L'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni integra fattispecie di reato previste dall'ordinamento nazionale.

Eventuali riprese televisive dei luoghi di lavoro per documentare attività o prestazioni solo per scopi divulgativi, scientifici, di comunicazione istituzionale o rappresentazione televisiva che vedano coinvolto il personale dipendente possono essere assimilate ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi e altre manifestazioni di pensiero. In tal caso, si applica la normativa nazionale sull'attività giornalistica, fermi restando i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione.

❖ OSPEDALI E LUOGHI DI CURA

Il controllo di ambienti sanitari ed il monitoraggio di pazienti ricoverati in particolari Unità Operative o ambienti, stante la natura particolare delle diverse categorie di dati che possono essere in tal modo trattati, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati, secondo i principi di necessità di cui al capitolo 4.

Considerata la natura particolare di queste categorie di dati personali, l'installazione e l'utilizzo degli impianti di ripresa nell'ambito di luoghi di cura deve garantire che il trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

I Delegati interni al trattamento dati devono garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (personale medico, infermieristico, tecnico, etc.) e incaricati al trattamento dei dati personali attraverso un sistema di videosorveglianza.

Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conviventi, conoscenti) di ricoverati in reparti dove non sia permesso agli stessi di recarsi personalmente, ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente, previo protocollo operativo, che sarà redatto dal responsabile della UU.OO., Delegato interno del trattamento dei dati, sentito il parere dell'U.O.C. Privacy – Trasparenza ed Integrità e del DPO.

Le eventuali riprese effettuate nell'ambito della psicoterapia sono soggette alla richiesta di consenso a parte del paziente. Nel modulo di consenso deve essere specificamente riportata l'autorizzazione al trattamento dei dati tramite ripresa audiovisiva delle sedute.

Al fine di garantire la necessaria riservatezza del paziente, i monitor riservati al controllo o destinati ai familiari devono essere posizionati in ambienti separati e normalmente non accessibili al pubblico.

Eventuali riprese effettuate ai fini della formazione possono essere compiute solo previa autorizzazione del Titolare, nonché informativa, consenso e liberatoria da parte degli interessati.

Le immagini idonee a rilevare lo stato di salute non devono essere comunque diffuse. In tale quadro va assolutamente evitato il rischio di diffusione delle immagini di persone malate su monitor collocati in locali liberamente accessibili al pubblico

Il mancato rispetto di quanto sopra stabilito comporta l'applicazione delle sanzioni amministrative stabilite nel GDPR, oltre la possibile integrazione di reati stabiliti dalla normativa nazionale.

CAPITOLO 9
DIRITTI DEGLI INTERESSATI

CAP. 9

❖ DIRITTI DEGLI INTERESSATI

Ai sensi del GDPR, all'interessato sono assicurati diversi diritti, in particolare:

a) accedere ai dati che lo riguardano (mediante apposito modello pubblicato sul sito aziendale);
b) verificare le finalità, le modalità e la logica del trattamento;
c) ottenere l'interruzione di un trattamento illecito, la cancellazione dei propri dati o la limitazione del trattamento degli stessi a determinate finalità (mediante apposito modello pubblicato sul sito aziendale).

Il Titolare, garantisce l'effettivo esercizio dei diritti dell'interessato, secondo le seguenti modalità:

1) l'Interessato, previa verifica dell'identità ed entro il periodo stabilito per la conservazione, può richiedere per iscritto l'accesso alle registrazioni che lo riguardano. L'eventuale accesso a registrazioni, riferite direttamente o indirettamente a terzi, sarà oggetto di apposito bilanciamento degli interessi da parte del Titolare, acquisito il parere dall'U.O.C. Privacy – Trasparenza ed Integrità e del DPO;
2) i dati sono estratti a cura dell'Incaricato e possono essere comunicati direttamente al richiedente mediante la visione delle registrazioni e, se vi è richiesta, si provvede alla duplicazione di tali registrazioni su adeguato supporto;

3) la visione e l'estrazione delle rilevazioni è gratuita per l'interessato; qualora, tuttavia, a seguito di questa operazione non risulti l'esistenza di dati che riguardano l'Interessato, potrà essergli addebitato un contributo spese, ai sensi del GDPR.

Ulteriori e più specifiche indicazioni sono delineate nella relativa procedura aziendale sui rapporti con gli interessati, cui si rimanda.

CAPITOLO 10
VIOLAZIONI DEL TRATTAMENTO

CAP. 10

❖ NOTIFICA DELLA VIOLAZIONE E REGISTRO DELLE VIOLAZIONI DEL TRATTAMENTO (RINVIO)

Si rimanda alla relativa procedura conservata presso il Titolare del trattamento per tutte le indicazioni in caso di violazione del trattamento dei dati personali.

CAPITOLO 11
NORME FINALI E DI RINVIO

CAP. 11

❖ NUOVE INSTALLAZIONI

L'installazione di nuovi impianti, così come l'incremento di nuove telecamere all'interno dei singoli impianti, avviene secondo quanto specificato al precedente art. 5, ovvero previa formale richiesta formulata dalle Direzioni Mediche di Presidio Ospedaliero, anche su indicazione delle UU.OO.CC. e UU.OO.SS.DD., ciascuna per il proprio ambito di competenza.
La richiesta, adeguatamente motivata e relazionata, viene inoltrata dalle direzioni Mediche di Presidio, al Titolare che si riserverà una ulteriore valutazione, all'U.O.C. Tecnico Patrimoniale ed all'U.O.C. Privacy – Trasparenza ed Integrità, e deve contenere i seguenti elementi:

a) le finalità perseguite, specificando le motivazioni che rendono proporzionale l'installazione di telecamere, rispetto all'effettivo grado di rischio;
b) l'area interessata, al fine di consentire la valutazione tecnica circa il numero, la dislocazione e la tipologia delle telecamere da installare;
c) se le immagini dovranno essere solo rilevate o anche registrate;
d) l'eventuale necessità di conservare le immagini per un periodo superiore alle 24 ore, specificandone le speciali esigenze.

La richiesta di installazione delle videocamere ed il conseguente trattamento di dati personali dovrà rispondere ai principi di liceità, di necessità e di proporzionalità e dovrà avvenire nel rispetto dall'art. 4, l. 300/1970 e s.m.i., "Statuto dei Lavoratori".

La U.O.C. Tecnico Patrimoniale attraverso i Delegati interni al trattamento dati, coordinerà le fasi di installazione del sistema di videosorveglianza richiesto, anche in raccordo con l'eventuale Responsabile Esterno che procederà alla relativa attivazione e successiva manutenzione. Questi ultimi assicureranno l'acquisizione e la installazione della cartellonistica conforme alle disposizioni di legge in materia vigenti, oltreché assicurarsi che le operazioni poste in essere siano conformi alla normativa di settore.

❖ ELENCO DEGLI IMPIANTI

Il Titolare detiene, presso la U.O.C. Tecnico Patrimoniale un apposito elenco inerente gli impianti di videosorveglianza, nel quale sono riportate le strutture presso cui sono posizionate le videocamere, il loro numero, se prevedono o meno la registrazione delle immagini e l'eventuale tempo di conservazione delle medesime.

Periodicamente ed almeno ogni sei mesi, la U.O.C. Tecnico Patrimoniale trasmette l'elenco aggiornato degli impianti di videosorveglianza installati presso l'Azienda alla U.O.C. Privacy – Trasparenza ed Integrità e alle DD.MM.OO.

L'elenco è accessibile alle Organizzazioni Sindacali.

La U.O.C. Tecnico Patrimoniale ha il compito, altresì, della conservazione dell'archivio della documentazione tecnica, afferente gli impianti di videosorveglianza, con indicazione delle modalità di ripresa degli stessi e la loro mappatura, e della documentazione riguardante i contratti di appalto, i protocolli, i verbali di sopralluogo condotti, la rendicontazione fatta dai Responsabili esterni del trattamento per la videosorveglianza e di tutto ciò che attiene alla corretta applicazione della normativa di settore.

❖ SANZIONI

In caso di inosservanza delle disposizioni in materia di videosorveglianza, si applicano le sanzioni previste dalla normativa vigente che saranno poste a carico del Titolare e del Direttore e/o del Dirigente Responsabile della struttura in cui è stata rilevata l'infrazione.

❖ PUBBLICAZIONE ED AGGIORNAMENTO

La presente procedura è stata adottata dal Titolare del trattamento, su proposta del DPO, e condivisa con l'U.O.C. Privacy – Trasparenza ed Integrità.

La suddetta procedura entra in vigore il giorno successivo alla sua approvazione e sostituisce in revisione la precedente. Il suo contenuto è soggetto ad aggiornamento periodico.

La sua diffusione, a cura dell'U.O.C. Privacy – Trasparenza ed Integrità, avverrà nelle seguenti forme: attraverso la rete informatica interna e la pubblicazione sul sito aziendale.

È fatto obbligo a chiunque spetti di osservarlo.

❖ NORMA DI RINVIO

Per quanto non espressamente previsto dal presente regolamento, si applicano le disposizioni di legge e i provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali che regolamentano la materia in oggetto.