

**INDICE**

1	OGGETTO ED AMBITO DI APPLICAZIONE.....	2
2	NORMATIVA DI RIFERIMENTO.....	2
3	DEFINIZIONI.....	2
4	FINALITÀ E PRINCIPI GENERALI DEL TRATTAMENTO.....	3
4.1	FINALITÀ DI SICUREZZA E TUTELA DEL PATRIMONIO AZIENDALE.....	4
4.2	FINALITÀ DI DIAGNOSI E CURA.....	4
4.3	BASE GIURIDICA.....	4
5	SOGGETTI DEL TRATTAMENTO.....	5
5.1	TITOLARE DEL TRATTAMENTO.....	5
5.2	RESPONSABILE INTERNO PRIVACY PER LA VIDEOSORVEGLIANZA.....	5
5.3	INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI DEL SISTEMA DI VIDEOSORVEGLIANZA.....	6
5.4	RESPONSABILE ESTERNO EX ART. 28 REGOLAMENTO EUROPEO 2016/679.....	7
5.5	AMMINISTRATORE DI SISTEMA.....	7
6	TUTELA DEI LAVORATORI.....	8
7	TUTELA DELLA RISERVATEZZA NEI LUOGHI DI CURA.....	8
8	CONSERVAZIONE DEI DATI.....	9
9	MISURE DI SICUREZZA E DPIA.....	9
10	IMPIANTO DI VIDEOSORVEGLIANZA.....	10
10.1	PROCEDURA PER NUOVA INSTALLAZIONE.....	10
10.2	UBICAZIONE.....	11
10.3	CARATTERISTICHE TECNICHE.....	11
11	ACCESSO AI DATI.....	12
12	INFORMATIVA.....	12
13	DIRITTI DEGLI INTERESSATI.....	13
14	CANCELLAZIONE DEI DATI.....	13
15	ACCERTAMENTO DI ILLECITI ED INDAGINI GIUDIZIARIE O DI POLIZIA.....	13
16	COMUNICAZIONE E DIFFUSIONE DEI DATI.....	14
17	TUTELA AMMINISTRATIVA E GIURISDIZIONALE.....	14
18	MODIFICHE E AGGIORNAMENTI.....	14
19	DISPOSIZIONI FINALI E DI RINVIO.....	14
20	DISTRIBUZIONE E ARCHIVIAZIONE.....	14
20.1	DISTRIBUZIONE.....	14
20.2	ARCHIVIAZIONE.....	15

Ed.	Rev.	Data	Descrizione delle modifiche	Redazione	Verifica di conformità al SGQ	Approvazione
01	00	27.11.2023	Prima emissione	Avv. M. Bazzana Ing. L. Ruggeri Ing. M. Bottazzi	Dott.ssa M.A. Rizzieri	Dr. M. Galavotti
01	01	15.09.2025	Seconda emissione	Avv. M. Bazzana Dott.ssa C. Mazzoli Dott.ssa F.L. Bianchi	Dott.ssa M.A. Rizzieri	Dott. C. Scolari Avv. G. Ceresetti

VERIFICA E CONFERMA DEI CONTENUTI

Ed.	Rev.	Data	Approvazione



1 OGGETTO ED AMBITO DI APPLICAZIONE

Con le presenti disposizioni attuative del regolamento aziendale in materia di protezione dei dati personali, l'ASST della Valcamonica (di seguito denominata anche "Azienda") intende disciplinare l'utilizzo dei sistemi di videosorveglianza presso le proprie strutture aziendali ospedaliere e territoriali, al fine di garantire che il trattamento dei dati personali effettuato mediante l'attivazione dei suddetti sistemi si svolga nel pieno rispetto dei diritti, delle libertà fondamentali, della dignità e della riservatezza delle persone fisiche.

Le presenti disposizioni disciplinano pertanto il trattamento dei dati personali effettuato con impianti di videosorveglianza (strumenti elettronici di rilevamento di immagini) in essere presso l'Azienda al momento in cui queste sono adottate, nonché le disposizioni a cui il titolare del trattamento dovrà attenersi per le nuove installazioni o per il rinnovamento di quelle esistenti.

Per tutto quanto non dettagliatamente disciplinato nel presente documento, si rinvia a quanto disposto dal Regolamento (UE) 2016/679 sulla protezione dei dati.

2 NORMATIVA DI RIFERIMENTO

La normativa di riferimento, a cui si rinvia per tutti gli aspetti non espressamente disciplinati dalle presenti disposizioni, è la seguente:

– Legge 20 maggio 1970, n. 300

"Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"(G.U. 27 maggio 1970, n. 131) c.d. "Statuto dei lavoratori";

– Decreto Legislativo 30 giugno 2003, n. 196

"Codice Privacy in materia di protezione dei dati personali" (G.U. 29 luglio 2003, 174 - Supplemento Ordinario n. 123), modificato ed integrato dal 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)", pubblicato sulla G.U. 04 settembre 2018 n. 205;

– Decreto Legislativo 9 aprile 2008 n. 81

"Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro";

– Provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010

"Provvedimento in materia di videosorveglianza" (G.U. n. 99 del 29 aprile 2010);

– 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 (di seguito anche RGPD);

– Linee guida 3/2019 sul trattamento di dati attraverso apparecchiature video adottate dal Comitato Europeo per la protezione dei dati il 29/01/2020 (EDPB - Guidelines 3/2019 on processing of personal data through video devices);

– Regolamento Aziendale in materia di Protezione dei Dati Personali (di seguito anche "Regolamento Aziendale").

3 DEFINIZIONI

Ai fini delle presenti disposizioni attuative s'intende:

A) per "**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 a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

B) per "**dati appartenenti a categorie particolari**", i dati che rivelino 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. 9.1 Regolamento europeo 2016/679); le immagini di pazienti riprese negli ambienti sanitari ed in particolari reparti sono dati personali particolari;

C) per "**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;

D) per **"titolare del trattamento"**, l'Azienda Socio Sanitaria Territoriale della Valcamonica, nella persona del Direttore Generale pro-tempore cui competono le decisioni in ordine alle e finalità e ai mezzi del trattamento dei dati personali;

E) per **"responsabile della protezione dei dati"**, o **"RPD"**, o **"DPO"**, persona esperta nella protezione dei dati personali a cui sono affidate funzioni di supporto e controllo, consultive, formative ed informative affinché i dati personali siano trattati nell'Azienda in modo lecito, corretto e pertinente, nonché punto di contatto per l'Autorità di controllo e per l'interessato riguardo alle questioni connesse al trattamento di dati personali;

F) per **"responsabile del trattamento"** ex art. 28 del Regolamento europeo 2016/679, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

G) per **"amministratore di sistema"**, una o più figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e alle quali è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione;

H) per **"responsabile interno privacy"**, la persona fisica, legata da rapporto di servizio al titolare del trattamento e preposto dal medesimo al trattamento di dati personali al quale il titolare stesso, nell'ambito delle misure organizzative adottate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al RGPD, demanda alcune responsabilità previste nelle presenti disposizioni attuative: individuato dall'Azienda nella figura del responsabile pro-tempore di struttura complessa (SC) e struttura semplice dipartimentale (SSD);

I) per **"responsabile interno privacy per la videosorveglianza"** (di seguito anche responsabile della videosorveglianza), il responsabile interno privacy autorizzato dal titolare del trattamento ad accedere ai locali in cui sono situate le postazioni di controllo dei sistemi, ad utilizzare gli stessi, a prendere visione ed eventualmente trattare le immagini quando ciò sia necessario per perseguire le finalità indicate nelle presenti disposizioni attuative;

J) per **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare del trattamento e/o dai responsabili interni privacy;

K) per **"interessato"**, la persona fisica a cui si riferiscono i dati personali;

L) per **"informativa"** il documento con cui si informano gli interessati che stanno per accedere in una zona videosorvegliata, ai sensi dell'art. 13 del Regolamento (UE) 2016/679;

M) per **"comunicazione"**, il dare conoscenza dei dati personali a soggetti determinati in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

N) per **"diffusione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

O) per **"videosorveglianza"** il sistema o il dispositivo elettronico volto a riprendere, con o senza registrazione delle immagini, aree o zone delimitate. In concreto si distinguono le seguenti tipologie:

- ripresa con visione delle immagini in tempo reale senza registrazione;
- ripresa con visione delle immagini in tempo reale, con registrazione delle stesse;
- ripresa con registrazione delle immagini, senza visione delle stesse in tempo reale.

Per ulteriori definizioni si rinvia a quanto previsto dall'art. 4 del Regolamento (UE) 2016/679.

4 FINALITÀ E PRINCIPI GENERALI DEL TRATTAMENTO

Il trattamento dei dati personali è effettuato a seguito dell'attivazione di un impianto di videosorveglianza, posizionato presso i presidi e le strutture aziendali indicati rispettivamente nei moduli M GPD 025 "Elenco delle telecamere e delle zone videosorvegliate per finalità di sicurezza e tutela del patrimonio" e M GPD 026 "Elenco delle telecamere e delle zone videosorvegliate per finalità di diagnosi e cura".

Il trattamento dei dati personali attraverso i sistemi di videosorveglianza è effettuato nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, dei cittadini e dei lavoratori, in ottemperanza ai principi di liceità, necessità, proporzionalità, esattezza, minimizzazione dei dati (pertinenza e non eccedenza), limitazione della finalità, limitazione della conservazione, integrità e riservatezza, dettati dalla normativa vigente in materia di protezione dei dati personali (art. 5 RGPD).



L'Azienda attua un sistema di videosorveglianza finalizzato esclusivamente allo svolgimento delle proprie attività istituzionali, ovvero:

- per garantire la sicurezza del patrimonio aziendale, mobiliare ed immobiliare e la protezione delle persone che, a vario titolo, accedono e/o sostano negli ambienti interni alle strutture ospedaliere ed ambulatoriali;
- per il perseguimento di finalità di diagnosi e cura delle persone che si avvalgono delle prestazioni erogate dall'Azienda.

4.1 FINALITÀ DI SICUREZZA E TUTELA DEL PATRIMONIO AZIENDALE

Al fine di perseguire le finalità di sicurezza delle persone e tutela del patrimonio aziendale, l'Azienda installa sistemi di videosorveglianza presso zone soggette a concreti pericoli o per le quali ricorre un'effettiva esigenza di deterrenza, di monitoraggio degli accessi o sia necessario garantire la sicurezza delle persone presenti nonché la tutela del patrimonio aziendale. L'obiettivo è quello di garantire alti standard di sicurezza, a tutela dei degenti e degli esercenti le professioni sanitarie e socio-sanitarie nell'esercizio delle loro funzioni, a contrasto dei fenomeni di aggressione, atti di violenza e/o altri reati contro la persona.

Gli impianti di videosorveglianza sono attivati quando altre misure siano ponderatamente valutate insufficienti o inattuabili o risultino inefficaci altri idonei accorgimenti, quali ad esempio: controlli da parte degli addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi ecc.

L'attività di videosorveglianza deve avvenire nel rispetto dei suddetti principi di necessità e proporzionalità in relazione alla scelta delle modalità di ripresa e dislocazione delle apparecchiature, nonché alle varie fasi del trattamento stesso che deve riguardare sempre dati pertinenti e non eccedenti rispetto alle finalità perseguite.

4.2 FINALITÀ DI DIAGNOSI E CURA

Al fine di monitorare e tutelare la salute dei pazienti, l'eventuale controllo di ambienti sanitari ed il monitoraggio di pazienti ricoverati e/o soggetti a terapia per finalità di diagnosi e cura, data la natura particolare della maggior parte dei dati che vengono raccolti e, se del caso, trattati, deve limitarsi ai casi di effettiva necessità, circoscrivendo le riprese a locali predeterminati.

La ripresa (sola rilevazione e non registrazione) per finalità di diagnosi e cura e l'eventuale conseguente trattamento dei dati particolari si svolge nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

L'accesso a tali immagini è consentito esclusivamente al personale sanitario, salvo quanto previsto dagli artt. 7 e 11 delle presenti disposizioni attuative.

4.3 BASE GIURIDICA

Il trattamento di dati personali avviene in modo lecito in quanto è necessario per le seguenti ragioni:

- per l'esecuzione di un compito di interesse pubblico e connesso all'esercizio di pubblici poteri (art. 6, par. 1 lett. e) RGPD);
- per finalità di diagnosi e cura quando effettuato in ambienti sanitari e per il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad esempio unità di rianimazione, reparti di isolamento, pronto soccorso, laboratori di analisi, ecc.) (art. 9, par. 2 lett. h) RGPD);
- per motivi di interesse pubblico rilevante (art. 9, par. 2 lett. g) RGPD), in quanto idoneo a tutelare la sicurezza delle persone, del patrimonio aziendale e a verificare e, se del caso, prevenire la commissione di illeciti e reati ed a garanzia della sicurezza e dell'ordine pubblico;
- per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (art. 9, par. 2 lett. b) RGPD).

L'uso dei dati personali nell'ambito di cui trattasi non necessita, pertanto, del consenso degli interessati.

L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite (limitazione della finalità), registrando o rilevando (a seconda della finalità) le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti (minimizzazione dei dati e rispetto dei principi di pertinenza non eccedenza). Il trattamento dei dati personali avviene nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento al diritto alla protezione dei dati personali e all'identità personale, in modo da garantirne un'adeguata sicurezza e protezione da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o dal danno accidentale, anche mediante l'adozione di specifiche misure tecniche o organizzative (integrità e



riservatezza). La localizzazione delle telecamere e le modalità di ripresa sono, quindi, stabilite in modo conseguente.

L'impianto di videosorveglianza non può essere utilizzato per effettuare controlli sull'attività lavorativa dei dipendenti.

L'impianto di videosorveglianza non può essere utilizzato per finalità statistiche, nemmeno se consistenti nella raccolta aggregata di dati.

L'impianto di videosorveglianza non può essere utilizzato per altre finalità non previste nelle presenti disposizioni attuative.

5 SOGGETTI DEL TRATTAMENTO

5.1 TITOLARE DEL TRATTAMENTO

Il titolare del trattamento dei dati relativi ai sistemi di videosorveglianza è l'ASST della Valcamonica in persona del proprio Direttore Generale pro-tempore.

Al titolare compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza adottate.

5.2 RESPONSABILE INTERNO PRIVACY PER LA VIDEOSORVEGLIANZA

Il responsabile interno privacy della videosorveglianza, è nominato con atto del Direttore Generale (M GPD 021), per le attività di installazione, configurazione, manutenzione degli apparati di videosorveglianza, per quelle attinenti al profilo di autorizzazione, nonché, nell'ambito dei sistemi che prevedono la registrazione delle immagini, per l'esecuzione di operazioni di estrazione, duplicazione e conversione delle immagini stesse.

Il responsabile della videosorveglianza, designato ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003 è scelto tra i soggetti che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle presenti disposizioni attuative e delle disposizioni di legge vigenti in materia, con particolare riferimento al profilo relativo alla sicurezza, riservatezza e tutela dei diritti dell'interessato. I compiti affidati al responsabile della videosorveglianza devono essere specificati per iscritto, in sede di designazione.

Il responsabile della videosorveglianza ha l'obbligo di attenersi a quanto previsto dalla normativa vigente in tema di trattamento dei dati personali, al regolamento aziendale in materia di privacy ed alle presenti disposizioni attuative.

A titolo esemplificativo e non esaustivo, è onere del responsabile provvedere a:

- individuare e nominare per iscritto gli incaricati del trattamento, dando loro le idonee istruzioni;
- richiedere al responsabile pro-tempore di struttura complessa (SC) e struttura semplice dipartimentale (SSD) l'aggiornamento periodico dei nominativi degli operatori delle UU.OO. interessate dalla videosorveglianza tramite la compilazione del relativo modulo approvato dall'Azienda;
- rispettare gli obblighi di riservatezza e segretezza delle informazioni di cui viene a conoscenza nel corso del trattamento dei dati;
- evitare la comunicazione di dati per scopi diversi da quelli perseguiti con l'installazione dell'impianto e per finalità diverse da quelle autorizzate, salvo il caso di richieste dell'Autorità Giudiziaria;
- garantire che l'accesso alle immagini non avvenga ad opera di personale non autorizzato;
- vigilare sul rispetto delle istruzioni impartite agli incaricati;
- verificare il rispetto da parte degli incaricati degli obblighi di riservatezza;
- dare istruzioni ed adeguata formazione ai soggetti incaricati per il corretto trattamento dei dati personali, proponendo un apposito piano di formazione per i nuovi incaricati;
- adottare e rispettare le misure di sicurezza indicate dal titolare del trattamento al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità di raccolta, così come previsto dalla vigente normativa, eseguendo controlli periodici, con cadenza almeno annuale;
- vigilare sul corretto funzionamento dell'impianto di videosorveglianza e sull'utilizzo secondo finalità lecite indicate nella normativa vigente e dalle presenti disposizioni;
- verificare che le telecamere siano sistemate in modo da limitare l'angolo di ripresa all'area da videosorvegliare;
- verificare la corretta custodia dei monitor e delle apparecchiature del sistema di videosorveglianza;
- adottare le necessarie cautele per assicurare la segretezza delle credenziali di autenticazione per l'accesso alle immagini in caso di registrazione;
- evadere le richieste di informazioni eventualmente pervenute da parte dell'Autorità Garante in materia



- di protezione dei dati personali, nei termini e secondo le modalità contenute nelle richieste;
- provvedere su richiesta delle autorità giudiziarie o di polizia a fare copia delle immagini registrate per le stesse autorità nei casi previsti dalla legge;
- comunicare al titolare del trattamento eventuali nuovi trattamenti da intraprendere nel rispetto della procedura di cui al successivo punto 10;
- relativamente ai sistemi di videosorveglianza che effettuano registrazione di immagini, provvedere a supervisionare le procedure di cancellazione/distruzione dati raccolti, nel caso in cui venga meno la finalità del trattamento ed il relativo obbligo di conservazione, ed ogni ed altra qualsivoglia attività espressamente delegata dal titolare del trattamento;
- collaborare con l'Autorità di controllo e segnalare una eventuale violazione di dati (data breach) al titolare del trattamento ed al responsabile della protezione dei dati immediatamente e comunque entro 12 ore dal momento in cui siano venuti a conoscenza.

5.3 INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI DEL SISTEMA DI VIDEOSORVEGLIANZA

Il responsabile della videosorveglianza, designa e nomina per iscritto, con apposita lettera di incarico (M GPD 022), gli incaricati, ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003, in numero sufficiente a garantire la gestione del servizio di videosorveglianza, individuando diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore.

Gli incaricati sono nominati tra i soggetti che per stato di servizio, specifiche attitudini, esperienza, capacità ed affidabilità forniscono idonea garanzia di riservatezza nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

Gli incaricati del materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del titolare del trattamento e del responsabile stesso, utilizzando gli impianti nei casi in cui sia indispensabile per gli scopi perseguiti. La sola ripresa di immagini, senza registrazione delle stesse, non comporta elaborazione del dato, fermo restando che la visione di immagini comporta comunque un trattamento di dati personali.

In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sulle presenti disposizioni attuative.

Il responsabile della videosorveglianza, i responsabili interni privacy e gli incaricati hanno l'obbligo di verificare che le operazioni di utilizzo e trattamento dei dati siano svolte nel rispetto delle norme vigenti e del regolamento aziendale in materia di tutela dei dati personali ed esclusivamente per gli scopi descritti sopra nonché il dovere di impedire che gli stessi, in caso di registrazione, siano divulgati a soggetti estranei all'attività di trattamento, salvo i casi d'intervento e/o richiesta da parte degli organi di Autorità Giudiziaria.

Il responsabile interno per la videosorveglianza, unitamente agli incaricati, sono gli unici ad accedere ai locali in cui sono situate le postazioni di controllo dei sistemi, ad utilizzare gli stessi, a prendere visione e a trattare le immagini quando ciò sia necessario per perseguire le finalità indicate nel presente documento.

Le classi di incaricati al trattamento dei dati personali relativi alla videosorveglianza sono:

- i portinai ubicati agli accessi dell'Azienda esclusivamente per il controllo accessi e comando cancelli elettrici;
- il personale sanitario e tecnico dell'UO ove sono installati i sistemi di videosorveglianza.

L'incaricato al trattamento, oltre ad attenersi alle specifiche istruzioni ricevute al momento della designazione ricevuta ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003 e ss.mm.ii., in relazione all'espletamento delle proprie mansioni all'interno dell'Azienda, ha l'obbligo di:

- trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle funzioni attribuitegli, in modo lecito e secondo correttezza mantenendo l'assoluta riservatezza e segretezza sulle informazioni di cui vengano a conoscenza nel corso delle operazioni del trattamento;
- effettuare la raccolta, l'elaborazione e la registrazione dei dati esclusivamente per lo svolgimento delle proprie mansioni e nei limiti delle finalità indicate nelle presenti disposizioni attuative;
- accedere ai dati nel rispetto delle misure di sicurezza adottate dal titolare del trattamento, in particolare non danneggiarli, alterarli, modificarli e soprattutto non diffonderli;
- controllare l'integrità ed il buon funzionamento dell'impianto di videosorveglianza;
- evitare che all'apparato ove vengono registrate le immagini acceda personale non autorizzato;



- vigilare, per quanto possibile, sul personale addetto alla pulizia dei locali, affinché venga inibita qualsivoglia forma di assunzione o rilevamento di dati;
- custodire con cura i monitor e l'apparecchiatura per la registrazione onde evitare la distruzione o la perdita di dati;
- custodire con cura le chiavi per l'accesso ai locali e agli armadi ove sono collocati i supporti di memorizzazione e gestione delle immagini registrate;
- adottare le necessarie cautele per la custodia delle credenziali di autenticazione di accesso al sistema di videosorveglianza ricevute e assicurarne la segretezza;
- segnalare al titolare del trattamento e al responsabile della videosorveglianza eventuali problemi applicativi rispetto all'attuazione e all'adempimento degli obblighi previsti dalla normativa privacy vigente;
- segnalare al titolare del trattamento, al responsabile della videosorveglianza ed al responsabile della protezione dei dati una eventuale violazione dei dati (data breach) immediatamente e comunque non oltre 12 ore da quando siano venuti a conoscenza.

5.4 RESPONSABILE ESTERNO EX ART. 28 REGOLAMENTO EUROPEO 2016/679

Le società incaricate dall'ASST della Valcamonica di effettuare la realizzazione degli interventi di manutenzione ordinaria e straordinaria hardware e software, comprensiva degli interventi necessari su dispositivi e software di archiviazione e di gestione del sistema di videosorveglianza, sono nominate dal titolare del trattamento quali responsabili esterni del trattamento dei dati con apposito atto scritto ai sensi dell'art. 28 Regolamento europeo 2016/679.

I rapporti con i responsabili esterni, ex art. 28 Regolamento europeo 2016/679, sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli stati membri.

I responsabili esterni del trattamento dei dati sono tenuti a fornire al titolare del trattamento l'elenco degli eventuali altri Responsabili del trattamento (c.d. sub-responsabili) e degli amministratori di sistema eventualmente nominati, e a tenerli costantemente aggiornati.

Il responsabile esterno dà formale comunicazione all'Azienda dei nominativi degli addetti alla manutenzione. Tali addetti hanno l'obbligo al segreto sulle immagini che eventualmente dovessero visionare nell'esercizio del loro lavoro.

5.5 AMMINISTRATORE DI SISTEMA

Nei sistemi di videosorveglianza installati che prevedono la registrazione di immagini, l'amministratore di sistema specificatamente nominato per la videosorveglianza ha il compito di impostare e gestire un sistema di autenticazione informatica per il responsabile della videosorveglianza e per i soggetti incaricati al trattamento di dati personali effettuato con strumenti di videosorveglianza, conforme a quanto previsto dal Regolamento privacy aziendale, dalle presenti disposizioni attuative, dal Regolamento europeo 2016/679 e dalla normativa vigente in materia di protezione dei dati personali.

L'amministratore di sistema, in particolare, avrà il compito di:

- garantire che i sistemi di videosorveglianza siano a circuito chiuso, in cui l'archiviazione delle immagini registrate non sia interconnessa con altri sistemi logici o altri archivi e non possa essere trasmessa in dispositivi remoti, ad eccezione del caso in cui ci si avvalga di una ditta esterna, nominata responsabile esterno del trattamento;
- attribuire al responsabile della videosorveglianza ed a ciascun incaricato al trattamento, per i compiti di rispettiva competenza, un codice identificativo personale per l'utilizzazione dell'impianto; uno stesso codice non potrà, neppure in tempi diversi, essere assegnato a persone diverse;
- assegnare e gestire il sistema di autenticazione informatica e quindi, fra le altre, generare, sostituire, invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i codici identificativi personali da assegnare a ciascun incaricato al trattamento dati;
- disporre ogni opportuna misura e ogni adeguata verifica, per evitare che soggetti non autorizzati possano avere accesso agli archivi delle parole chiave se leggibili;
- controllare che il periodo di conservazione delle immagini sia limitato al tempo stabilito dalle presenti disposizioni, salvo casi eccezionali dovuti all'intervento dell'Autorità Giudiziaria o della Polizia Giudiziaria;
- adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; tali registrazioni devono comprendere i riferimenti temporali e la



descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

- assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery), anche automatici nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS);
- provvedere affinché gli elaboratori del sistema informativo siano protetti contro il rischio di intrusione ad opera di programmi diretti a danneggiare il sistema, mediante idoneo software la cui efficacia ed aggiornamento siano verificati con cadenza almeno semestrale;
- monitorare costantemente lo stato di sicurezza di tutti i processi di elaborazione dati di cui sopra, mantenendo aggiornati tutti i supporti hardware e software e, se del caso, comunicando al titolare del trattamento tutte le attività da porre in essere al fine di garantire un adeguato livello di sicurezza in proporzione alla tipologia e quantità dei dati personali trattati;
- assistere il titolare del trattamento, il responsabile della videosorveglianza ed il responsabile della protezione dei dati per quanto concerne l'analisi dei rischi e l'adempimento previsto dal Regolamento europeo 2016/679 relativo alla valutazione di impatto (DPIA - Data Protection Impact Assessment);
- segnalare al titolare del trattamento, al responsabile della videosorveglianza ed al responsabile della protezione dei dati una eventuale violazione dei dati (data breach) immediatamente e comunque entro e non oltre 12 ore da quando sia venuto a conoscenza.

Il titolare del trattamento accerta la puntuale osservanza, da parte del responsabile della videosorveglianza, dei soggetti incaricati e dell'amministratore di sistema, delle disposizioni di legge e delle presenti disposizioni attuative.

6 TUTELA DEI LAVORATORI

Nell'attività di videosorveglianza è fatto obbligo di rispettare il divieto di controllo a distanza dell'attività lavorativa (ex art. 4, comma 1, L. n. 300/1970), pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di controllare la produttività e l'efficienza nello svolgimento dell'attività lavorativa o verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro.

A tal fine, nella dislocazione delle telecamere sono state tenute in considerazione le seguenti misure di tutela:

- le telecamere non inquadrano bagni, spogliatoi, sale sindacali, spazi ricreativi;
- non sono state posizionate telecamere all'interno degli uffici;
- le telecamere non sono dotate di sistemi di rilevazione sonora (eccetto quelle delle sale operatorie integrate, che vengono gestite dagli operatori stessi) che possano configurare l'ipotesi di intercettazione di comunicazioni e conversazioni.

Inoltre:

- tutto il personale è stato informato dell'adozione del sistema di videosorveglianza per le finalità indicate;
- la presenza delle telecamere è segnalata mediante affissione di appositi cartelli posizionati nelle immediate vicinanze dei luoghi ripresi;
- il responsabile della videosorveglianza e gli incaricati sono stati resi edotti delle norme di legge e delle disposizioni del Garante per la protezione dei dati personali in relazione ai trattamenti dei dati in materia di videosorveglianza.

In caso di impianti e di apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive, dalla sicurezza del lavoro ovvero dalla tutela del patrimonio aziendale, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, si procederà alla loro installazione soltanto previo accordo con le rappresentanze sindacali aziendali. In mancanza di accordo, gli impianti e gli strumenti potranno essere installati previa autorizzazione dell'Ispettorato Territoriale del Lavoro competente per territorio, ai sensi dell'art. 4, comma 1, L. 20 maggio 1970 n. 300 (Statuto dei lavoratori).

7 TUTELA DELLA RISERVATEZZA NEI LUOGHI DI CURA

Data la natura particolare dei dati che possono essere raccolti nei presidi ospedalieri e nei luoghi di cura, l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. unità di rianimazione, reparti di isolamento, pronto soccorso, laboratori di analisi, astanterie, ecc.), devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati.



In tali casi occorre inoltre adottare tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione di quanto prescritto nel provvedimento generale del Garante per la protezione dei dati personali del 8 aprile 2010.

Alle immagini rilevate per le predette finalità possono avere accesso solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (congiunti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto.

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse e va assolutamente evitato il rischio di diffusione delle immagini di persone malate.

Sono escluse dalla disciplina delle presenti disposizioni attuative le registrazioni audio/video effettuate nell'ambito di particolari trattamenti di cura, per le quali è necessaria l'acquisizione del consenso da parte del paziente (es. sedute di psicoterapia, videoriprese in sede di intervento chirurgico, riprese e registrazioni per altre attività medico-scientifiche e didattico, di medicina legale, ecc.).

8 CONSERVAZIONE DEI DATI

Gli impianti di videosorveglianza possono effettuare ripresa in tempo reale con o senza registrazione delle immagini a seconda della specifica finalità per la quale sono installati. Tale distinzione è specificatamente indicata rispettivamente nelle tabelle di cui ai **moduli M GPD 025 e M GPD 026**.

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 tempo non superiore a quello strettamente necessario al soddisfacimento delle finalità dell'impianto e del livello di rischio delle aree soggette al controllo.

L'Azienda ha individuato, per le finalità di cui alle presenti disposizioni attuative, un periodo di conservazione delle immagini di 72 ore dalla rilevazione.

L'Azienda ha, altresì, definito, per specifiche telecamere posizionate nella struttura, l'estensione del periodo di conservazione fino a 7 giorni dalla rilevazione, tenuto conto della collocazione e della finalità per cui sono installate, derivante dalla necessità di garantire maggiore sicurezza in zone non presidiate o zone di largo afflusso di pubblico per il rischio concreto di furto e/o altro illecito, anche alla luce dell'assenza o dell'esiguità del personale che possa monitorare gli eventi e quindi gestire la sicurezza in tempo reale, con conseguente difficoltà di tempestiva segnalazione. Si tratta di telecamere posizionate in luoghi in cui non è possibile prevedere altre misure di sicurezza, in quanto ponderatamente valutate insufficienti o inattuabili o inefficaci. La particolare esigenza di conservazione delle immagini registrate fino a 7 giorni deriva inoltre della necessità emersa negli anni di gestire eventuali richieste provenienti dall'Autorità Giudiziaria ovvero da Forze di Pubblica sicurezza in maniera adeguata fornendo agli stessi opportuna collaborazione, tenuto conto delle tempistiche tecniche per fornire un adeguato riscontro.

Nell'elencazione delle telecamere presenti nella struttura, di cui ai moduli sopra richiamati, risulta indicata anche la specifica tempistica di conservazione delle immagini registrate.

In tutti i casi in cui sia necessario procedere ad un allungamento dei tempi di conservazione per un periodo superiore a 7 giorni, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante per la protezione dei dati personali.

I tempi di conservazione qui disciplinati non potranno essere, quindi, superati salvo l'ipotesi di specifica richiesta investigativa da parte dell'Autorità Giudiziaria o della Polizia Giudiziaria o per esigenze di conservazione della prova processuale e per l'esercizio o la difesa di un diritto in sede giudiziale e stragiudiziale.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Il rispetto dei termini di conservazione delle registrazioni e della programmazione delle tempistiche di registrazione e cancellazione delle immagini, secondo le modalità previste dalle presenti disposizioni, è assicurato dal responsabile interno privacy per la videosorveglianza.

Le immagini rilevate per finalità di cura e diagnosi non possono essere registrate e conseguentemente conservate.

9 MISURE DI SICUREZZA E DPIA

Gli impianti di videosorveglianza ed i dati con essi raccolti devono essere salvaguardati, mediante adeguate e preventive misure di sicurezza riducendo al minimo i rischi di distruzione e di perdita, anche



accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità di raccolta, anche in relazione alla trasmissione delle immagini.

È compito del titolare del trattamento, dei responsabili interni privacy e della videosorveglianza, dell'amministratore di sistema, nonché dei soggetti autorizzati ed incaricati, adottare e rispettare tutte le misure di sicurezza ritenute adeguate come previsto dal Regolamento europeo 2016/679, tra le quali le misure tecniche ed organizzative di seguito indicate:

A) garantire che tutti i locali in cui viene effettuato il monitoraggio della videosorveglianza e dei filmati siano protetti contro l'accesso non sorvegliato da parte di terzi in modo che solo gli operatori autorizzati possano visualizzarli. Infatti l'accesso ai locali ove sono ubicati i sistemi di visualizzazione deve essere consentito solamente ai soggetti responsabili interni privacy e agli incaricati, designati e autorizzati al trattamento, nonché a soggetti esterni addetti all'assistenza ed alla manutenzione degli impianti, nominati responsabili del trattamento ex art. 28 RGPD;

B) predisporre un sistema di controllo accessi (user-id, password) che preveda credenziali di autenticazione distinte per profili di abilitazione in relazione ai compiti espletati: visualizzazione delle immagini, manutenzione degli impianti, estrazione delle immagini, nel caso il sistema sia predisposto per la registrazione;

C) assicurare che eventuali verifiche tecniche effettuate da incaricati esterni siano espletate in presenza dei soggetti interni alla struttura organizzativa;

D) adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici, in relazione alle operazioni compiute sulle immagini, che prevedano l'indicazione dei relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato, comunque non inferiore a sei mesi. Le registrazioni degli accessi logici (access log) devono garantire caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste, ovvero per verificare eventuali abusi e/o violazioni della riservatezza dei dati;

E) predisporre misure tecniche ed organizzative adeguate per la cancellazione/sovrascrittura in forma automatica delle registrazioni al termine previsto;

F) provvedere alla distruzione dei supporti deputati alla memorizzazione delle immagini, nel caso in cui debbano essere sostituiti per eccessiva usura o guasti irreparabili, in modo da renderli inutilizzabili, affinché non possano essere recuperati i dati in essi presenti;

G) assicurare che le immagini riprese e registrate contenenti dati particolari non riportino l'indicazione di nominativi o comunque di dati diretti ad identificare i soggetti ripresi nelle registrazioni;

H) adottare sistemi di cifratura delle registrazioni;

I) garantire che le chiavi per l'accesso ai locali ove sono ubicati gli apparati informatici dedicati alla memorizzazione e gestione delle immagini siano custodite a cura del responsabile interno per la videosorveglianza o dagli incaricati al trattamento;

L) collocare i monitor degli impianti di videosorveglianza in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate;

M) garantire che i server/dispositivi di registrazione siano sorretti da gruppo di continuità;

N) provvedere a documentare mediante l'annotazione in un apposito registro (cartaceo od informatico) a cura del responsabile interno per la videosorveglianza l'esercizio dei diritti da parte degli interessati;

O) programmare iniziative periodiche di formazione rivolte ai soggetti designati ed autorizzati al trattamento.

Il titolare del trattamento, prima di dare inizio al trattamento di videosorveglianza, coadiuvato dal responsabile della videosorveglianza e dal responsabile interno privacy del servizio su cui è o deve essere installato l'impianto, e con il parere del responsabile della protezione dei dati, effettua la valutazione di impatto sulla protezione dei dati (DPIA), volta a valutare la proporzionalità e necessità del trattamento delle immagini, analizzare i rischi a cui esso espone gli interessati, indicando e ponendo in essere misure idonee per eliminarli o mitigarli (art. 35 RGPD).

Qualora le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato, l'impianto non potrà essere installato.

10 IMPIANTO DI VIDEOSORVEGLIANZA

10.1 PROCEDURA PER NUOVA INSTALLAZIONE

L'installazione degli impianti o la modifica degli stessi è autorizzata dal Direttore Generale a seguito di proposta motivata avanzata dai responsabili di ciascuna Unità Operativa/Presidio/Servizio, in concerto



con il responsabile interno privacy per la videosorveglianza e sentito il parere del responsabile della protezione dei dati.

La procedura per una nuova installazione si articola nella seguenti fasi:

- 1 Ricevuta la richiesta, il titolare del trattamento valuterà, obiettivamente e con un approccio selettivo, se l'utilizzazione ipotizzata sia conforme ai principi di liceità, necessità, proporzionalità, esattezza, minimizzazione dei dati, limitazione della finalità, limitazione della conservazione, integrità e riservatezza, effettuando un bilanciamento attento ed equilibrato degli interessi contrapposti, tenuto conto dei diritti e le libertà fondamentali dei cittadini e degli utenti. In tale attività si avvarrà della collaborazione del Direttore Medico di Presidio, ovvero del responsabile della SC o SSD competente, dal responsabile della videosorveglianza oltre che del responsabile dei servizi informativi.
- 2 La medesima richiesta sarà trasmessa al responsabile della protezione dei dati che supporterà il titolare del trattamento nella valutazione.
- 3 Ogni nuova installazione deve essere espressamente autorizzata dal titolare del trattamento o da un suo delegato, anche in ordine alla scelta delle caratteristiche dell'impianto che devono essere rispondenti allo scopo perseguito.
- 4 In merito alle nuove installazioni il titolare del trattamento darà informazione alle OO.SS, salvo i casi di cui all'art. 4 dello Statuto dei lavoratori.

L'installazione, la configurazione, il profilo di autorizzazione, la modifica, la sostituzione e la manutenzione degli impianti di videosorveglianza sono effettuate dal responsabile della videosorveglianza con proprio personale o tramite ditte esterne. Il responsabile della videosorveglianza avrà la responsabilità di curare la conformità degli impianti alle misure adeguate di sicurezza previste dalla normativa vigente in materia di protezione dei dati personali, direttamente, in caso di realizzazione in proprio, o previa attestazione dell'appaltatore (in caso di realizzazione in appalto).

In caso di installazione di nuovi impianti, all'esito della procedura sopra descritta, il responsabile della videosorveglianza aggiorna i **moduli M GPD 025 e M GPD 026**.

10.2 UBICAZIONE

Le telecamere posizionate per garantire la sicurezza del patrimonio aziendale, mobiliare ed immobiliare, e per la protezione delle persone sono posizionate in punti nevralgici come descritto nel **modulo M GPD 025**.

Le telecamere posizionate per finalità di diagnosi e cura sono posizionate ed hanno le caratteristiche descritte nel **modulo M GPD 026**.

Tali impianti potranno essere eventualmente ampliati secondo gli sviluppi futuri del sistema.

I **moduli M GPD 025 e M GPD 026** contengono gli elenchi aggiornati delle aree interessate dalle riprese delle telecamere dei sistemi di videosorveglianza. Gli elenchi devono contenere le seguenti informazioni: denominazione della sede aziendale, indirizzo, ubicazione della telecamera, zona di ripresa e funzione, presenza di registrazione o rilevazione, caratteristiche tecniche dell'installazione, durata della conservazione delle immagini per gli impianti che effettuano anche la registrazione.

Tali elenchi dovranno essere resi disponibili al Garante per la protezione dei dati personali ed ai suoi delegati nelle attività di vigilanza ed ispezione e sono resi accessibili alle organizzazioni sindacali.

10.3 CARATTERISTICHE TECNICHE

I sistemi di videosorveglianza sono a circuito chiuso; per gli impianti che effettuano anche la registrazione, l'archiviazione delle immagini registrate non è interconnessa con altri sistemi logici, con altri archivi o banche dati e può essere convogliata in dispositivi anche periferici. Le apparecchiature di registrazione, in tal caso, devono essere custodite in luoghi protetti (es. armadi rack o similari) e non sono accessibili senza autenticazione con credenziali di accesso individuali e tracciabili.

L'impianto non deve contemplare:

- la raccolta di immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali oppure con codici identificativi di carte elettroniche o con dispositivi che rendono identificabile la voce o le immagini;
- l'indicizzazione o digitalizzazione delle immagini tale da rendere possibile una ricerca automatizzata o nominativa;
- sistemi dotati di software che permettono l'associazione di immagini a dati biometrici o che permettono di riprendere, registrare e segnalare automaticamente comportamenti ed eventi anomali.

Le caratteristiche tecniche degli impianti di videosorveglianza, sono riportate nei documenti del



produttore custoditi presso l'ufficio tecnico e potranno essere oggetto di aggiornamento in caso di sostituzione dell'impianto.

11 ACCESSO AI DATI

Nei sistemi di videosorveglianza predisposti per la registrazione delle immagini, il responsabile della videosorveglianza, d'intesa con l'amministratore di sistema, individua diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, che deve essere in possesso di credenziali di autenticazione che permettono di effettuare, a seconda dei compiti attribuiti, unicamente le operazioni di propria competenza, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

In ogni caso, l'accesso alle immagini da parte delle persone autorizzate al trattamento dei dati si limita alle attività oggetto della sorveglianza. Eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione.

L'accesso alle immagini e ai dati personali è consentito:

- al titolare del trattamento, al responsabile interno privacy per la videosorveglianza, ai responsabili interni privacy dell'UO/Servizio eventualmente interessato dall'attività di sorveglianza, nonché agli incaricati dello specifico trattamento;
- ai preposti alle indagini dell'Autorità Giudiziaria o di Polizia;
- all'amministratore di sistema dell'Azienda e alla ditta fornitrice dell'impianto nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione;
- all'interessato, debitamente autorizzato, in quanto oggetto delle riprese. Nel caso di accesso ai dati da parte dell'interessato questi avrà visione solo delle immagini che lo riguardano direttamente.

Per le telecamere installate per finalità di diagnosi e cura, non rientrano tra le persone estranee non autorizzate i terzi legittimati (congiunti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto.

Eventuali accessi di persone diverse da quelle innanzi indicate devono essere autorizzati, per iscritto, dal responsabile della videosorveglianza o dal titolare del trattamento.

Per i sistemi di videosorveglianza installati che effettuano anche la registrazione di immagini, il sistema dovrà essere fornito di procedure di tracciamento degli accessi (login e logout), che saranno conservati per un congruo periodo non inferiore a sei (6) mesi.

Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito "registro degli accessi" derivante dalla registrazione dei file di log ricavati dal sistema. Qualora il sistema non abbia questa funzione sarà necessario annotare su apposito registro da parte degli incaricati i seguenti dati relativi agli accessi:

- la data e l'ora dell'accesso;
- l'identificazione del terzo autorizzato;
- i dati per i quali si è svolto l'accesso;
- gli estremi e la motivazione dell'autorizzazione all'accesso;
- le eventuali osservazioni dell'incaricato;
- la sottoscrizione del medesimo.

12 INFORMATIVA

Tutti coloro che accedono ai presidi ospedalieri ed alle strutture dell'ASST della Valcamonica, sono opportunamente informati dell'esistenza di impianti di videosorveglianza nell'area in cui stanno per transitare.

L'obbligo di informativa è adempiuto con un modello semplificato di informativa "minima" (**Schede S GPD 020A, S GPD 020B, S GPD 020C e S GPD 021**), ossia con l'esposizione di cartelli indicanti la presenza nell'area di una o più telecamere.

I cartelli devono essere posizionati ad "altezza occhi" e ad una distanza ragionevole dai luoghi monitorati per consentire agli interessati di essere avvisati della videosorveglianza prima di entrare nel raggio di azione della telecamera.

Essi devono avere un formato ed un posizionamento tale da essere chiaramente visibili in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia attivo in orario notturno.

I cartelli raffiguranti la videosorveglianza riportano i seguenti dati:



- identità del titolare del trattamento;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento;
- la base giuridica;
- se l'attività è limitata alla sola rilevazione o si estende anche alla registrazione delle immagini;
- i diritti degli interessati;
- le modalità di accesso all'informativa estesa.

L'accesso all'informativa estesa (S GPD 019) è garantito agli interessati tramite la pubblicazione della stessa sul sito web aziendale all'indirizzo <https://www.asst-valcamonica.it> all'interno della sezione "Privacy e Protezione dei Dati Personali".

L'informativa estesa sulla videosorveglianza può essere esplicitata anche con l'utilizzo di QR code apposti sui cartelli contenenti l'informativa "minima".

13 DIRITTI DEGLI INTERESSATI

In relazione al trattamento dei dati personali il titolare del trattamento assicura all'interessato l'effettivo esercizio dei diritti stabiliti dagli articoli 12 e seguenti del RGPD nonché dall'art. 15 del regolamento aziendale in materia di trattamento dei dati personali. I diritti dell'interessato potranno essere esercitati nelle modalità descritte nelle disposizioni attuative adottate dall'Azienda e denominate "Istruzioni relative all'esercizio dei diritti in materia di protezione dei dati personali dell'interessato ai sensi degli artt. 12-22 del Regolamento (UE) 2016/679", pubblicate sul sito web aziendale all'indirizzo <https://www.asst-valcamonica.it> all'interno della sezione "Privacy e Protezione dei Dati Personali".

Per ciascuna delle richieste di cui al presente articolo può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, secondo le modalità previste dalla normativa vigente.

In riferimento alle immagini registrate, non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.

L'istanza dell'interessato deve, altresì, indicare a quale impianto di videosorveglianza si fa riferimento ed il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa: nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, ne dovrà essere data comunicazione al richiedente, così come nell'ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione.

Il responsabile della videosorveglianza o un incaricato sarà tenuto ad accertare l'effettiva esistenza delle immagini nei limiti del termine di conservazione delle stesse previsti dalle presenti disposizioni, e ne darà comunicazione al richiedente. 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.

La risposta alla richiesta di accesso a dati deve riguardare i dati attinenti alla persona richiedente e può comprenderne eventualmente altri, riferiti a terzi, solo nei limiti previsti dalla normativa vigente.

Decorsi i termini di conservazione indicati al punto 8 delle presenti disposizioni, la richiesta di accesso non potrà essere soddisfatta.

Qualora l'interessato sia vittima di reati, le eventuali registrazioni, ove l'impianto sia a ciò predisposto, saranno rilasciate su richiesta dell'Autorità Giudiziaria. I dati registrati si intendono a disposizione dell'Autorità Giudiziaria per i fini istituzionali di tali organi, previa richiesta scritta.

14 CANCELLAZIONE DEI DATI

Per i sistemi di videosorveglianza che effettuano anche la registrazione di immagini, decorso il termine di conservazione indicato al punto 8 delle presenti disposizioni attuative, i dati dovranno essere cancellati in modo automatico con le modalità, stabilite dal responsabile della videosorveglianza d'intesa con l'amministratore di sistema, che saranno ritenute più efficaci, ovvero anche effettuando nuove registrazioni su quelle precedenti, affinché possa essere conseguito l'effetto di renderle non più utilizzabili.

15 ACCERTAMENTO DI ILLECITI ED INDAGINI GIUDIZIARIE O DI POLIZIA

Per i sistemi di videosorveglianza installati che effettuano anche la registrazione, in caso di rilevazioni d'immagini relative a fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza,



o del patrimonio aziendale, l'incaricato o il responsabile interno privacy per la videosorveglianza provvede a darne comunicazione senza ritardo all'Autorità competente, provvedendo, nel contempo, alla conservazione delle immagini su appositi supporti.

Alle immagini raccolte ai sensi del presente articolo possono accedere, per l'espletamento delle relative indagini, solo gli appartenenti all'Amministrazione Giudiziaria, le persone da essi espressamente autorizzate e gli organi di Polizia.

Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino una copia delle riprese effettuate, devono presentare un'istanza scritta e motivata indirizzata al titolare del trattamento, salvo non sia in essere apposita convenzione.

16 COMUNICAZIONE E DIFFUSIONE DEI DATI

La comunicazione dei dati personali acquisiti mediante il sistema di videosorveglianza da parte del responsabile interno privacy per la videosorveglianza, a favore di altri soggetti autorizzati, è ammessa quando necessaria ed esclusiva per lo svolgimento delle funzioni istituzionali.

È in ogni caso fatta salva la comunicazione e la diffusione di dati richiesti in conformità alla legge, da Forze di Polizia, dall'Autorità Giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

17 TUTELA AMMINISTRATIVA E GIURISDIZIONALE

La mancata osservanza degli obblighi previsti dalle presenti disposizioni attuative comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla legge, di sanzioni amministrative o penali.

In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della L. 7 agosto 1990 n. 241, è il responsabile della videosorveglianza.

18 MODIFICHE E AGGIORNAMENTI

I contenuti delle presenti disposizioni attuative dovranno essere aggiornati nei casi di variazioni delle normative in materia di trattamento dei dati personali, gerarchicamente superiori. Gli eventuali atti normativi, atti amministrativi del Garante per la protezione dei dati personali o atti regolamentari aziendali, dovranno essere immediatamente recepiti.

19 DISPOSIZIONI FINALI E DI RINVIO

Le presenti disposizioni attuative entrano in vigore dalla data di approvazione da parte del Direttore Generale e saranno rese disponibili sulla rete intranet aziendale, nonché pubblicate sul sito web aziendale all'indirizzo <https://www.asst-valcamonica.it> all'interno della sezione privacy.

Per tutto quanto non disciplinato dalle presenti disposizioni attuative si fa rinvio alle leggi vigenti, ai provvedimenti attuativi delle medesime, alle decisioni del Garante per la protezione dei dati personali, al regolamento aziendale in materia di trattamento dei dati personali e ad ogni altra normativa, speciale, generale, nazionale e comunitaria in materia di protezione e trattamento dei dati personali nell'ambito della videosorveglianza.

20 DISTRIBUZIONE E ARCHIVIAZIONE

20.1 DISTRIBUZIONE

Il documento "Gestione della documentazione SGQ" P GEN 001 definisce le modalità di distribuzione della presente informazione documentata.

La conoscenza della presente informazione documentata e la sua implementazione nell'articolazione organizzativa è assicurata dalla Leadership e dal RQ con incontri verbalizzati.

L'accesso alle registrazioni è controllato dal RQ al fine di evitare che soggetti non direttamente coinvolti nelle attività possano modificare o alterare l'ordine e la modalità di conservazione e rintracciabilità.

Le registrazioni sono archiviate in un luogo dedicato, idoneo e facilmente identificabile.

La presente informazione documentata è trasmessa a:

- Direzione Strategica
- RUO tramite i RQ
- Ufficio Qualità.

Copia cartacea a nessuno.

**20.2 ARCHIVIAZIONE**

DENOMINAZIONE DOCUMENTO	CODICE DOCUMENTO	ALL.	ALTRI DOC. CORRELATI	CLASS.*	LUOGO ARCHIVIAZIONE	REFERENTE ARCHIVIAZIONE	TEMPO CONSERVAZIONE*	REFERENTE SCARTO
Disposizioni attuative per l'installazione e l'utilizzo di impianti di videosorveglianza	I GPD 004	//	//	1.7.03	Avvocatura	RPD	10	RPD
Informativa sul trattamento dei dati personali ai sensi dell'art. 13 Regolamento (UE) 2016/679 (RGPD)	S GPD 019	X	//	1.7.03	Avvocatura	RPD	10	RPD
Informativa sul trattamento dei dati personali ai sensi dell'art. 13 Regolamento (UE) 2016/679 - videosorveglianza per finalità di sicurezza e tutela del patrimonio	S GPD 020A S GPD 020B S GPD 020C	X	//	1.7.03	Avvocatura	RPD	10	RPD
Informativa sul trattamento dei dati personali ai sensi dell'art. 13 Regolamento (UE) 2016/679 - videosorveglianza per finalità di diagnosi e cura	S GPD 021	X	//	1.7.03	Avvocatura	RPD	10	RPD
Elenco delle telecamere e delle zone videosorvegliate per finalità di sicurezza e tutela del patrimonio	M GPD 025	X	//	1.7.03	Avvocatura	RPD	10	RPD
Elenco delle telecamere e delle zone videosorvegliate per finalità di diagnosi e cura	M GPD 026	X	//	1.7.03	Avvocatura	RPD	10	RPD

* Riportare la classificazione e il tempo di conservazione come indicato nel "Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia" Revisione 04 e ss.mm.ii.

I dati personali dell'interessato oggetto del trattamento saranno conservati per il periodo necessario a rispettare i termini di conservazione stabiliti nel Massimario di Scarto approvato dalla Regione Lombardia attualmente in vigore e ss.mm.ii., ovvero, qualora ve ne sia l'esigenza, per un ulteriore periodo strettamente necessario:

- *al perseguimento delle finalità dell'attività istituzionale gestita dall'Azienda;*
- *a difendere i propri diritti in sede giudiziaria o dinanzi ad autorità giurisdizionali;*
- *ad adempiere correttamente agli obblighi previsti da norme di legge o di regolamento, cui è soggetta l'Azienda.*