REGOLAMENTO IN MATERIA DI VIDEOSORVEGLIANZA

SCOPO E ORGANIZZAZIONE DEL DOCUMENTO

L'ASL di TARANTO, in seguito denominata anche A.S.L. Taranto, per le proprie peculiarità organizzative, la dislocazione territoriale e le caratteristiche strutturali degli edifici, nell'intento di voler garantire una maggiore attenzione alla tutela delle persone (che a vario titolo frequentano gli ambienti delle Strutture aziendali ed accedono alle stesse) e alla sicurezza interna ed esterna agli edifici nonché degli impianti, **intende dotarsi, nel rispetto dei principi di necessità e proporzionalità, di sistemi di videosorveglianza nei diversi spazi in cui si svolgono le attività istituzionali.**

Si precisa che le immagini riguardanti le persone, qualora rendano possibile l'identificazione del soggetto al quale si riferiscono, costituiscono dati personali. La videosorveglianza dà luogo, pertanto, a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.

Il presente Regolamento disciplina il funzionamento dei sistemi di videosorveglianza installati in prossimità degli accessi e all'interno delle Strutture dell'A.S.L. e garantisce che il trattamento dei dati personali registrati dai sistemi di videocamera si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

In particolare l'A.S.L. effettua attività di videosorveglianza esclusivamente per:
1. garantire la sicurezza del patrimonio aziendale e delle persone che, a vario titolo, frequentano gli ambienti delle strutture aziendali o che accedono agli stessi nonché la tutela dell'integrità fisica del personale dipendente durante lo svolgimento delle sue funzioni (art.2087 del c.c.*);
2. il perseguimento di finalità di cura delle persone che si avvalgono delle prestazioni erogate dalla ASL (c.d. videocontrollo per monitoraggio pazienti).

**1) Il datore di lavoro deve adottare tutte le misure idonee a prevenire sia i rischi insiti all'ambiente di lavoro, sia quelli derivanti da fattori esterni e inerenti al luogo in cui tale ambiente si trova, atteso che la sicurezza del lavoratore è un bene di rilevanza costituzionale che impone al datore di anteporre al proprio profitto la sicurezza di chi esegue la prestazione.*

Articolo 1 – Definizioni

Ai fini del presente Regolamento, si intende:
- 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;
- 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;
- per «*banca dati*», il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree interessate dalle riprese;
- per «*profilazione*», qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- per «*pseudonimizzazione*», il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a 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 a una persona fisica identificata o identificabile;
- per «*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;
- per «*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;
- per «*incaricato del trattamento*», la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del responsabile del trattamento;

- per «*interessato*», la persona fisica cui si riferiscono i dati personali oggetto di trattamento;
-per *"DPO"* (*Data Protection Officer*) è una figura introdotta dal Regolamento Generale sulla protezione dei dati 2016/679(c.d. GDPR) con il compito di osservare, valutare ed organizzare la gestione del trattamento dei dati personali. Il DPO ha molteplici mansioni e, per questo, il Regolamento Europeo Privacy ha previsto che questo ruolo sia indipendente e abbia grande autonomia decisionale. In primo luogo, l'Officer per la protezione dei dati fornisce consulenza al responsabile della conservazione e informa tutte le figure coinvolte, sia in merito alla normativa, sia riguardo alle soluzioni tecniche adottate per rispettare gli standard imposti.
- per «*terzo*», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- per «*violazione dei dati personali*», la 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;
- per «*comunicazione*», il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per «*diffusione*», il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- per «*dato anonimo*», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Articolo 2 – SCOPO E ORGANIZZAZIONE DEL DOCUMENTO

2.1 OGGETTO ED AMBITO D'APPLICAZIONE

1. La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configurano un trattamento di dati personali.

2. Il trattamento di dati personali attraverso sistemi di videosorveglianza da parte dell'ASL avviene esclusivamente nell'ambito dello svolgimento delle funzioni istituzionali.

3. La determinazione della dislocazione delle videocamere e delle modalità di ripresa e il trattamento dei dati raccolti vengono effettuati in osservanza dei seguenti principi:
- *Principio di liceità*: il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connes-

so all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ossequio al disposto di cui all'art. 6, Paragrafo 1, lett. e), RGPD. [1];
- *Principio di necessità*: in applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD[2], il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati;
- *Principio di proporzionalità*: la raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento;
Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere;
- *Principio di finalità*: ai sensi dell'art. 5, Paragrafo 1, lett. b), RGPD [3], i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità.

[1] 1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (C40) e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; (C45, C46)

[2] 1. I dati personali sono: (C39) c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

[3] 1. I dati personali sono: (C39) c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

4. Laddove, per la natura dei dati trattati, per le modalità di trattamento o per gli effetti che il trattamento può determinare, emergano rischi specifici per i diritti e le libertà fondamentali degli interessati, L'A.S.L. procederà all'effettuazione della Valutazione d'impatto sulla protezione dei dati, in conformità a quanto previsto all'art. 35 RGPD [4].

2.2. PRINCIPI

2.2.1 Videosorveglianza Esterna

La necessità dell'A.S.L. di permettere un'attività di videosorveglianza all'esterno delle strutture Sanitaria, risponde alla necessità di svolgere al meglio il proprio ruolo istituzionale di tutela del patrimonio, rappresenta una soluzione infrastrutturale necessaria secondo gli standard presenti nella letteratura internazionale ed è una misura proporzionale al fatto che può permettere la tutela delle aree esterne degli edifici ai fini della

[4] **Articolo 35 Valutazione d'impatto sulla protezione dei dati (C84, C89-C93, C95)**

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.
7. La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.
11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

sicurezza e tutela del Patrimonio. La necessità di dotare alcune delle Strutture**,** che per la loro conformità e per la loro posizione presentano delle criticità oggettive, di un tale sistema deve rispondere ai principi etici di "liceità", "necessità", "proporzionalità" e ''finalità" previsti dalla normativa vigente in materia.
2.2.1.1 Finalità: l'installazione di sistemi di rilevazione delle immagini da parte dell'ASL risponde alle seguenti finalità, determinate, esplicite e legittime:

- prevenire fatti criminosi agendo come deterrente
- favorire la repressione in quanto può fornire i dati rilevati nei luoghi ove avvengono
- sorvegliare in presa diretta zone che di volta in volta presentano particolari elementi di criticità o in concomitanza di eventi rilevanti per l'ordine e la sicurezza dei luoghi esterni agli edifici
- rassicurare gli utenti attraverso una chiara comunicazione sulle zone sorvegliate
- tutelare la sicurezza esterna degli Edifici
- supportare le forze di polizia in tutte le attività di prevenzione e controllo

L'accesso alle centrali di controllo, alle immagini ed ai dati da esse raccolti e trattati è consentito esclusivamente ai:

- Titolari del Trattamento dei dati dell'ASL, S.S.D. Ingegneria Clinica e dei Sistemi Informativi Aziendali, DPO e Responsabile Esterno del Trattamento
- Incaricati addetti ai servizi ad essi designati
- Alle forze dell'ordine per lo svolgimento delle loro attività investigative e per fini istituzionali.

2.2.2 Videosorveglianza Interna

L'esigenza dell'A.S.L. presuppone la necessità di realizzare un sistema di videosorveglianza interno che rispetti i seguenti parametri:
• Determinato, dalle esigenze specifiche;
• Legittimo, coerente allo scopo Istituzionale dell'A.S.L.;
• Pertinente, con i compiti istituzionali dell'ASL.

Tali scopi, pertanto, non potranno che essere quelli della
- tutela della salute dei pazienti (prevenzione, diagnosi, cura e riabilitazione) e la loro sicurezza,
- il miglioramento complessivo della sicurezza all'interno delle Strutture sanitarie aziendali.

Lo scopo d'uso del sistema di videosorveglianza dovrà, pertanto, essere adeguatamente motivato anche con riferimento all'inattuabilità o all'insufficienza di altre misure.

Il provvedimento generale del Garante del 8.4.2010 in materia videosorveglianza prevede, infatti, l'obbligo che le ragioni che hanno determinato la scelta dell'installazione del sistema di videosorveglianza debbano essere adeguatamente documentate in un atto au-

tonomo, conservato presso il titolare 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 contestazioni.

2.2.2.1 Finalità

La videosorveglianza è finalizzata allo svolgimento delle funzioni istituzionali dell'A.S.L., tenuto conto delle esigenze derivanti dall'organizzazione aziendale. Il trattamento dei dati personali attraverso i sistemi di videosorveglianza è effettuato in ottemperanza al principio di liceità per garantire la sicurezza e la protezione di beni e persone, nonché per la prevenzione e l'efficace perseguimento dei reati.
In particolare le finalità principali sono:
1. protezione delle persone all'interno delle singole strutture aziendali e in particolare prevenzione delle aggressioni e/o di altri reati contro la persona;
2. prevenzione incendi e sicurezza del lavoro
3. sicurezza degli ambienti interni alle strutture aziendali;
4. tutela dei beni e persone e in particolare prevenzione dei reati contro il:
   - patrimonio dell'azienda
   - dei dipendenti
   - degli utenti

5. controlli difensivi diretti ad accertare la commissione dei reati. Pertanto, è necessario la possibilità di installare le telecamere nei seguenti punti rispettando i diritti di cui al successivo punto 2.2.2.1
A) Reception
B) Corridoi di transito
C) Aree comuni ad eccezione dei punti di ristoro
D) Ingressi / uscite ascensori
E) Ingressi / uscite locali tecnici
F) Uscite di emergenza/antincendio
G) Unità operative particolari quali la Rianimazione, Pronto Soccorso, Strutture e Servizi sanitari nei quali vi sono dei particolari ambienti riservati ai pazienti che per la loro patologia hanno necessità di essere monitorati h24 per particolare esigenza di cura e tutela della tutela degli stessi interessati.

L'attività di videosorveglianza deve avvenire nel rispetto del principio di necessità e proporzionalità nella scelta delle modalità di ripresa e dislocazione delle apparecchiature, nonché nelle varie fasi del trattamento stesso.

2.2.2.1 Tutela della riservatezza dei lavoratori

Nelle attività di sorveglianza è fatto obbligo di rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di

lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge).

Quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro e soprattutto del personale dipendente , vanno osservate le garanzie previste in materia di lavoro: e cioè, ai sensi dell'art. 4 della l. n. 300/1970 [5], gli impianti e le apparecchiature, dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, **possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali**. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

2.2.2.2 Tutela della riservatezza degli utenti negli ospedali e nei luoghi di cura

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (di cui alla precedente lettera G), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati.

Devono essere inoltre adottati 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 dal Garante per la Protezione dei Dati nei suoi provvedimenti emessi in materia di videosorveglianza.

In tali casi i Direttori/Dirigenti delle Unità operative interessate devono garantire che l'accesso alle immagini rilevate per le predette finalità sia riservato solo ed esclusivamente ai 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 (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (di cui alla precedente lettera G), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'im-

[5] *Art. 4. Impianti audiovisivi.*
1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.
2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.
3. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.
4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

magine solo del proprio congiunto o conoscente. Al fine di garantire la necessaria riservatezza del paziente, i monitor riservati al controllo o destinati alla visione da parte dei soggetti autorizzati di cui sopra devono essere posizionati in ambienti riservati e non accessibili al pubblico. Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse. In tale quadro, va assolutamente evitato il rischio di diffusione delle immagini di persone ricoverate o allettate su monitor collocati in locali liberamente accessibili al pubblico.

Le riprese effettuate nell'ambito della psicoterapia necessitano del previo consenso da parte del paziente il quale dovrà espressamente autorizzare il trattamento dei dati acquisiti nel corso delle sedute.

Le riprese aventi finalità scientifiche e/o formative devono essere espressamente autorizzate dalla Direzione Generale, in quanto Titolare dei trattamenti, e possono essere effettuate solo quando il paziente, dopo aver acquisito la relativa informativa, ha sottoscritto specifico consenso e liberatoria.

2.2.2.3 Modalità di richiesta installazione sistemi videosorveglianza

Il trattamento dei dati raccolti con i sistemi di videosorveglianza deve avvenire nel rispetto del "principio di necessità nel trattamento dei dati".

I sistemi ed i programmi informatici a supporto degli impianti di videosorveglianza devono essere configurati in modo tale da ridurre al minimo l'utilizzazione dei dati personali e dei dati identificativi quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi.

Gli stessi devono essere altresì conformati in modo tale da permettere l'identificazione dell'interessato solo in caso di necessità.

I dati personali trattati in violazione del principio di che trattasi non possono essere utilizzati. L'installazione di sistemi di video sorveglianza deve essere preceduta da una richiesta di autorizzazione alla Direzione Generale dell'ASL di Taranto, in quanto Titolare dei trattamenti, ed al DPO Aziendale il quale dovrà verificare la rispondenza del sistema di videosorveglianza al principio di necessità del relativo trattamento dei dati, e stabilire se sottoporre o meno alla verifica preliminare del garante sistemi particolari di video sorveglianza. Per la peculiarità delle attività sanitarie e dei servizi offerti dall'A.S.L. le immagini vengono conservate fino a 7 giorni, in quanto l'attività di videosorveglianza è finalizzata alla tutela di interessi meritevoli di una maggiore difesa, quali la sicurezza pubblica, tutela e sicurezza del personale operante "turnista"; tutela e sicurezza dei ricoverati. Così come è necessaria la conservazione delle immagini per almeno 7 gg. in quanto rientra nel caso di speciali esigenze di "proroga" dovuta a festività o chiusura di uffici.

Le immagini acquisite dalle unità di ripresa sono visualizzate su monitor collocati nelle aree di accettazione appositamente attrezzate garantendo la riservatezza e non accessibile al pubblico. L'accesso è consentito -per motivi di controllo e verifica- solo al Titolare, al DPO e al Responsabile esterno del Trattamento ed agli incaricati di quest'ultimo per lo svolgimento della loro attività e funzioni oltre al personale di pubblica sicurezza o di polizia giudiziaria. L'accesso di soggetti diversi da quelli indicati può avvenire solo in via eccezionale, per comprovata necessità in relazione alle finalità indicate nell'articolo 2 e previa autorizzazione del Titolare o del DPO.

Le immagini sono conservate su appositi server o supporti analoghi custoditi nel rispetto delle misure di sicurezza richieste dalla vigente normativa. I sistemi di videosorveglianza non conformi al principio di necessità, seppur non funzionanti, dovranno essere rimossi a cura dei Responsabili delle strutture in cui sono installati.

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

ARTICOLO 3 MODALITA' DI GESTIONE E SOGGETTI INTERESSATI: TITOLARE, RESPONSABILI, INCARICATI DEL TRATTAMENTO E DPO

1.Il Titolare dei trattamenti di dati personali effettuati mediante sistemi di videosorveglianza installati presso l'ASL stessa, intesa come persona giuridica, è rappresentato dal suo Legale Rappresentante, ovvero il Direttore Generale pro tempore. All'ASL compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

2. Il servizio oggetto del presente regolamento può essere gestito da responsabili esterni del trattamento a seguito del servizio in outsourcing che hanno presentato garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate assicurando la tutela dei diritti dell'interessato. A tal fine si è proceduto a disciplinare i trattamenti da parte dei Responsabili esterni mediante contratto ovvero atto giuridico che vincola gli stessi Responsabili esterni del trattamento al Titolare del trattamento ai sensi dell'art. 38, RGPD [6].

[6] **Articolo 38 Posizione del responsabile della protezione dei dati (C97)**
1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare

3. L'individuazione degli incaricati è effettuata per iscritto da parte del Responsabile Esterno del Trattamento e con modalità tali da consentire una chiara e puntuale definizione dell'ambito del trattamento consentito a ciascun Incaricato, specificando se il trattamento consiste nella sola visione delle immagini registrate e/o nell'accesso alle immagini registrate ed alla possibilità di estrazione delle stesse.

In ogni caso, prima dell'utilizzo degli impianti, gli incaricati dovranno essere istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.

Gli Incaricati procedono al trattamento attenendosi alle istruzioni impartite dal Responsabile esterno del Trattamento il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.

Le nomine degli incaricati al trattamento devono essere comunicate da parte del Responsabile esterno del trattamento al Titolare.

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- conservare i supporti informatici contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento delle proprie mansioni o funzioni istituzionali;
- custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare banche dati nuove senza autorizzazione espressa del Titolare del trattamento;
- conservare e trattare i dati rispettando le misure di sicurezza predisposte dall'ASL;

---

del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

- fornire al Designato, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Articolo 4 - Raccolta e trattamento dei dati

1. La raccolta dei dati avviene tramite videocamere aventi le caratteristiche tecniche descritte in un apposito documento (capitolato conservato agli atti della Direzione Generale). In ragione di sopraggiunte nuove implementazioni per effetto di novità tecnologiche e/o esigenze per rispondere alle finalità di cui al precedente articolo 2, il Titolare del trattamento dei dati provvederà a modificare il documento nel rispetto di quanto previsto dal presente Regolamento con comunicazione alle OO.SS., alle RSU, agli RLS e agli Organi competenti.

2. Le videocamere installate presso le sedi dell'A.S.L. consentono unicamente riprese video e non effettuano riprese audio. La registrazione delle immagini avviene con videocamere a immagine fissa. Le videocamere installate agli accessi e varchi delle strutture aziendali non saranno orientate sui lettori badge né, all'interno né sulle postazioni di lavoro.

3. Non vengono installate apparecchiature specificamente preordinate al controllo a distanza dell'attività del personale dipendente e di tutti coloro che operano a vario titolo nell'A.S.L., non saranno effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza, il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa o dell'attività diversa espletata. Laddove dai sistemi installati per le finalità sopra elencate derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, l'ASL adotta le garanzie previste dall'articolo 4, comma 1, della legge n. 300/1970 (v. precedente nota 4).

Articolo 5 – PROCEDURA DI INSTALLAZIONE, ATTIVAZIONE, DISATTIVAZIONE E FUORI USO DEI SISTEMI DI VIDEOSORVEGLIANZA

1. Procedura di installazione
L'A.S.L. ha affidato all'esterno la gestione dei sistemi di videosorveglianza attualmente in uso, distinguendo le attività in:
- manutenzione impianti esistenti;
-installazione e manutenzione nuovi impianti.

A tal fine, l'A.S.L. Taranto provvederà a nominare i responsabili esterni del trattamento provvedendo a fornire copia del presente regolamento, affinché l'attività assegnata sia svolta conformemente a quando ivi disposto.

I RESPONSABILI ESTERNI, ognuno per la propria competenza devono:
- provvedere per iscritto alla nomina degli incaricati che sono preposti all'utilizzo e alla gestione della videosorveglianza o videocontrollo e a comunicare i nominativi al Titolare ed al Data Protection Officer (DPO) Aziendale
- provvedere a dare istruzioni agli incaricati per il corretto trattamento dei dati
- adottare misure di sicurezza al fine di ridurre i rischi di distruzione o perdita anche accidentale di dati, accesso non autorizzato, trattamento non consentito
-far rispettare dai propri incaricati gli obblighi di segretezza e di non divulgazione dei dati di cui siano venuti a conoscenza.

Per l'installazione di nuovi impianti e per la modifica/sostituzione di quelli esistenti deve essere rispetta la seguente procedura:

1. La richiesta di attivazione/modifica/sostituzione di impianto, deve essere presentata dal responsabile della Struttura dove si chiede l'installazione/modifica dell'apparecchiatura e deve essere adeguatamente motivata ed in linea con il principio di proporzionalità secondo il quale l'attività di videosorveglianza è attivata solo nei luoghi in cui altre misure (es. sistemi di allarme, controllo fisici o logistici, misure di protezione agli ingressi) non siano sufficienti, attuabili o parimenti efficaci;
2. L'istanza va inviata a mezzo email alla Direzione Amministrativa al seguente indirizzo: direttoreamministrativo@asl.taranto.it ;
3. La richiesta viene valutata dal Direttore Amministrativo sentito il DPO Aziendale. Il DPO effettua le valutazioni di conformità alla normativa nazionale, al presente regolamento aziendale ed alle verifiche tecniche ed informatiche ed esprime il proprio parere che potrà essere:
   - **positivo** che potrà comprendere anche eventuali prescrizioni ed indicazioni in merito alle modalità, accorgimenti e/o procedure particolari da seguire per l'esecuzione dei lavori
   - **negativo** (purché motivato) ovvero si potrà richiedere chiarimenti indicando le criticità riscontrate in sede di verifica.
4. In caso di parere positivo, la richiesta è inoltrata all'Area Gestione tecnica, all'Area Gestione del Patrimonio ed alla S.S.D. Ingegneria Clinica e dei Sistemi Informativi Aziendali ognuno per la sua competenza.
5. In caso di richiesta di chiarimenti da parte del DPO Aziendale rivolta alla Struttura richiedente, questa dovrà fornire le osservazioni e sarà soggetto a nuovo parere di conformità secondo le procedure sopra previste.
6. La richiesta (n.d.r di attivazione/modifica/sostituzione di impianto) dovrà essere riscontrata entro 15 giorni lavorativi.

La materiale installazione dell'impianto avverrà a cura della ditta fornitrice dello stesso, (previo autorizzazione della Direzione Aziendale) e previo sopralluogo con i Responsabili del Trattamento esterni e con il D.P.O. Aziendale.

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

Chiunque autorizzi l'installazione di apparecchi di controllo a distanza senza il rispetto della presente procedura risponde dell'installazione a titolo personale incorrendo anche nella responsabilità disciplinare.

Alla Direzione Amministrativa (e/o al D.P.O) devono essere inoltrate ogni richiesta di estrapolazione di immagini, da parte delle Autorità, per consentire interventi autorizzativi alla società gestore delle apparecchiature. Di detti interventi il DPO provvede ad istituire apposito registro ove verranno riportati tutti gli accessi effettuati sulle apparecchiature (ivi compresi gli interventi di manutenzione ordinaria e straordinaria).

Procedura del fuori uso.
Il fuori uso può avvenire per due motivi:

A- Obsolescenza/non riparabilità della strumentazione in uso;
B- È cessato l'interesse di avere un impianto attivo in una data posizione ovvero presso le Strutture interessate.

Nel primo caso, la S.S.D. Ingegneria Clinica e dei Sistemi Informativi Aziendali, attraverso la società che gestisce la manutenzione, comunica alla Direzione Amministrativa ed al DPO Aziendale la proposta del fuori uso chiedendo la contestuale valutazione della sostituzione con un nuovo impianto.

Nel secondo caso, l'istanza del fuori uso deve essere inoltrata dalla Struttura che dichiari l'inutilità dell'impianto in quella posizione (es. Direttore Amministrativo, DPO Aziendale in caso di una sede dismessa ovvero nel caso di modifica della legislazione vigente; del Direttore Medico per un reparto trasferito in altri ambienti o del Direttore del Distretto o altra causa oggetto di valutazione per l'eventuale dismissione dell'impianto).

Articolo 6 - Misure di sicurezza

I dati raccolti mediante il sistema di videosorveglianza sono protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:
a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;
c) la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Ai sensi dell'art. 32, Paragrafo 2, RGPD [7], nel valutare l'adeguato livello di sicurezza, l'A.S.L. terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dall'A.S.L. stessa.

A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative che consentano al Titolare di verificare l'attività espletata da parte di chi accede alle immagini e/o controlla i sistemi di ripresa:
a) per quanto riguarda il periodo di conservazione delle immagini, così come già indicato nel precedente art. 2.2.2.3 dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, al rigoroso scadere del termine previsto;
b) nel caso di interventi derivanti da esigenze di manutenzione, si renderà necessario adottare specifiche cautele: in particolare, i soggetti incaricati di procedere a dette operazioni potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno in presenza dei soggetti dotati di credenziali di autenticazione ed abilitanti alla visione delle immagini;
c) gli apparati di ripresa digitali connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
d) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless.

Il Titolare, il DPO ed i Responsabili esterni del Trattamento vigilano sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvedono altresì ad istruire e formare gli incaricati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interessati.

Articolo 7– Accesso ai dati

L'accesso ai dati registrati ed alle loro immagini al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente:

[7] **Articolo 32 Sicurezza del trattamento (C83)** …..2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

a) alla società fornitrice dell'impianto ovvero al soggetto incaricato della manutenzione nei limiti strettamente necessari alle specifiche esigenze di funzionamento e manutenzione dell'impianto medesimo
b) all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta, secondo la procedura descritta al successivo art. 10. L'accesso da parte dell'interessato sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte del Titolare del trattamento, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti
c) ai soggetti legittimati all'accesso ai sensi e per gli effetti degli artt. 22 e ss. L. 241/90 [8] e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'art. 24, comma 7, L. 241/90 [9], l'accesso alle immagini sia necessario per curare o per difendere gli interessi

[8] **Art. 22 (Definizioni e princípi in materia di accesso)** (articolo così sostituito dall'art. 15 della legge n. 15 del 2005)
1. Ai fini del presente capo si intende:
a) per "diritto di accesso", il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi;
b) per "interessati", tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso;
c) per "controinteressati", tutti i soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza;
d) per "documento amministrativo", ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale;
e) per "pubblica amministrazione", tutti i soggetti di diritto pubblico e i soggetti di diritto privato limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o comunitario.
2. L'accesso ai documenti amministrativi, attese le sue rilevanti finalità di pubblico interesse, costituisce principio generale dell'attività amministrativa al fine di favorire la partecipazione e di assicurarne l'imparzialità e la trasparenza.
(comma così sostituito dall'art. 10, comma 1, legge n. 69 del 2009)
3. Tutti i documenti amministrativi sono accessibili, ad eccezione di quelli indicati all'articolo 24, commi 1, 2, 3, 5 e 6.
4. Non sono accessibili le informazioni in possesso di una pubblica amministrazione che non abbiano forma di documento amministrativo, salvo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, in materia di accesso a dati personali da parte della persona cui i dati si riferiscono.
5. L'acquisizione di documenti amministrativi da parte di soggetti pubblici, ove non rientrante nella previsione dell'articolo 43, comma 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al d.P.R. 28 dicembre 2000, n. 445, si informa al principio di leale cooperazione istituzionale.
6. Il diritto di accesso è esercitabile fino a quando la pubblica amministrazione ha l'obbligo di detenere i documenti amministrativi ai quali si chiede di accedere

[9] **Art. 24 (Esclusione dal diritto di accesso)** (articolo così sostituito dall'art. 16 della legge n. 15 del 2005)
1. Il diritto di accesso è escluso:
a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;
c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psico-attitudinale relativi a terzi.
2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.
3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.
4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.

giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto istante.

Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito "registro degli accessi" (cartaceo od informatico), conservato a cura dei Responsabili esterni del Trattamento, nel quale sono riportati ad opera degli incaricati:
• 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.

E' fatto divieto assoluto estrapolare parti di immagini registrate ovvero visionare le registrazioni se ciò non è previsto da una disposizione e/o un provvedimento motivato anche da parte della Autorità Giudiziaria.

Articolo 8- Comunicazione e diffusione

La comunicazione a soggetti pubblici dei dati personali acquisiti mediante i sistemi di videosorveglianza è ammessa solo se prevista da norma di legge o, nei casi previsti dalla legge o di regolamento. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgi-

---

5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.
6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:
a) quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale,
all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione;
b) quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
c) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;
d) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono;
e) quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.
7. Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale

mento di funzioni istituzionali, previa comunicazione al Garante nei termini e con le modalità previste all'art. 2-ter, comma 2, del D.Lgs. n. 196/2003 [10].

Sono fatte salve in ogni caso 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 ai sensi dell'art. 58, comma 2, del D. Lgs. n. 196/2003 [11]per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

La comunicazione e la diffusione devono essere in ogni caso autorizzate dal Titolare del trattamento ai sensi dell'art. 4 del presente Regolamento.

I dati non sono in nessun caso soggetti a diffusione generalizzata.

Articolo 9 - Informativa agli interessati

L'ASL informa gli interessati in ordine alla presenza negli spazi, aree ed ambienti aziendali anche aperti al pubblico di sistemi di videosorveglianza mediante l'affissione nelle zone interessate, in prossimità della videocamera, del modello semplificato di informativa "minima", indicante il Titolare del trattamento e le finalità perseguite, riportato in facsimile nell'allegato n. 1.

L'informativa deve essere collocata prima del raggio di azione della videocamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, potranno essere installati più cartelli informativi.

---

[10] **Art. 2-*ter*** (*Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*) 2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'art. 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

[11] **Art. 52** (*Dati identificativi degli interessati*) 2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.

3. L'A.S.L. mette a disposizione degli interessati sul proprio sito internet, mediante affissione in bacheche e presso gli sportelli destinati agli utenti, il testo completo dell'informativa, contenente tutti gli elementi di cui agli artt. 13 e 14 RGPD [12].

---

[12] **Articolo 13 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (C60-C62)**
1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce
all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.
Articolo 14 Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato (C60-C62)
1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.
2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
e) il diritto di proporre reclamo a un'autorità di controllo;
f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:
a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure

Articolo 10 - Diritti dell'interessato

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD [13], su presentazione di apposita istanza, ha diritto:
a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi
b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali
c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD[14], la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge,

---

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.
4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.
5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:
a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

[13]**Articolo 15 Diritto di accesso dell'interessato (C63, C64)**
1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.
3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

[14]**Articolo 17 Diritto alla cancellazione («diritto all'oblio») (C65, C66)**
1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati
d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD [15].

L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'ASL, ai sensi dell'art. 38, paragrafo 4, RGDP [16](i cui dati di contatto sono disponibili sul sito istituzionale dell'ASL nella sezione "Privacy") ovvero al Designato o direttamente al Titolare.

---

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

[15]**Articolo 21 Diritto di opposizione (C69, C70)**
1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

[16]**Articolo 38 Posizione del responsabile della protezione dei dati (C97)**
…4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
• il luogo, la data e la fascia oraria della possibile ripresa;
• l'abbigliamento indossato al momento della possibile ripresa;
• gli eventuali accessori in uso al momento della possibile ripresa;
• l'eventuale presenza di accompagnatori al momento della possibile ripresa;
• l'eventuale attività svolta al momento della possibile ripresa;
• eventuali ulteriori elementi utili all'identificazione dell'interessato.

Il Designato accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.

Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD (nota 13) , l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD (nota 13).

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.

Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Articolo 11 - Mezzi di ricorso, tutela amministrativa e tutela giurisdizionale

Per tutto quanto attiene al diritto di proporre reclamo o segnalazione al Garante, nonché con riferimento ad ogni altro profilo di tutela amministrativa o giurisdizionale, si rinvia integralmente a quanto disposto dagli artt. 77 e ss, RGPD e al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.

Per quanto non espressamente previsto dal presente Regolamento, si rinvia integralmente alle norme in materia di tutela dei dati personali (Regolamento UE Generale sulla Protezione dei Dati 2016/679 - RGDP; D. Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 101/2018; Garante per la protezione

dei dati personali - Provvedimento in materia di videosorveglianza 8 aprile 2010), nonché alla L. 300/1970. Provvedimenti del Garante in materia

Articolo 12- Entrata in vigore
Il presente Regolamento entra in vigore dal giorno della sua approvazione.