



REGIONE SICILIANA
Azienda Ospedaliera di Rilievo Nazionale e di Alta Specializzazione
"GARIBALDI"
Catania

DELIBERAZIONE N° 298 del 23 MAR. 2026

Proposta n. del

Oggetto: Approvazione e adozione del Regolamento sulla videosorveglianza e sull'uso dei dispositivi indossabili (c.d. bodycam) dell'ARNAS Garibaldi di Catania.

L'Istruttore

Dott. Ennio Romano

Il Direttore Amministrativo

Dott. Carmelo Fabio Antonio Ferrara

Registrazione Contabile

Budget Anno Conto Importo Aut.

NULLA OSTA, in quanto conforme alle norme di contabilità

Il Dirigente Responsabile

Settore Economico Finanziario e Patrimoniale

(dott. Giovanni Luca Roccella)

Nei locali della sede legale dell'Azienda, Piazza S. Maria di Gesù n. 5, Catania,

il Direttore Generale, Dott. Giuseppe Giammanco,

nominato con Decreto Presidenziale n.321/Serv 1°/S.G./2024

con l'assistenza del Segretario, **Dott.ssa Antonella Cinardo** ha adottato la seguente deliberazione

IL DIRETTORE AMMINISTRATIVO

VISTA la Legge n. 300/1970 – c.d. “*Statuto dei Lavoratori*”, come modificata dal D. Lgs.151/2015;

RICHIAMATI:

- il Decreto Legislativo 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)*”;
- il 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 (GDPR) nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*”;
- il D. Lgs. 30 giugno 2003 n. 196 recante il “*Codice in materia di protezione dei dati personali*”;

VISTO il Decreto Legge 1° ottobre 2024, n. 137, coordinato con la Legge di conversione 18 novembre 2024, n. 171, recante: «*Misure urgenti per contrastare i fenomeni di violenza nei confronti dei professionisti sanitari, socio-sanitari, ausiliari e di assistenza e cura nell'esercizio delle loro funzioni nonché di danneggiamento dei beni destinati all'assistenza sanitaria*»;

RITENUTO opportuno adottare formalmente il Regolamento Aziendale sulla videosorveglianza e sull'uso dei dispositivi indossabili (c.d. bodycam) (Allegato 1);

PRECISATO che il Regolamento è stato inviato alle OO.SS. della dirigenza e del comparto e, successivamente, in occasione degli incontri del 23/01/2026 e del 13/02/2026 il Regolamento è stato approvato dalle OO.SS.;

PRECISATO che l'ARNAS Garibaldi provvederà a effettuare una Valutazione d'Impatto sulla protezione dei dati ex art. 35 del Regolamento (UE) 2016/679 per assicurare misure idonee a garantire la sicurezza dei dati trattati;

PRECISATO che i dispositivi saranno utilizzati in via sperimentale nel Pronto Soccorso, nel Pronto Soccorso pediatrico e nel Pronto Soccorso di Ostetricia e Ginecologia per un periodo di anni due;

PRECISATO che dal presente atto deliberativo non scaturiscono oneri economici a carico dell'Azienda;

ACQUISITO il parere favorevole del Direttore Sanitario che viene espresso con la sottoscrizione del presente atto;

ATTESTATA la legittimità formale e sostanziale dell'odierna proposta e la sua conformità alla normativa disciplinante la materia trattata, ivi compreso il rispetto della disciplina di cui alla L. 190/2012

Propone

Per le motivazioni descritte in narrativa, che qui si intendono integralmente riportate e trascritte di:

Approvare e adottare il Regolamento Aziendale sulla videosorveglianza e sull'uso dei dispositivi indossabili (c.d. bodycam) (Allegato 1);

Dare atto che dal presente atto deliberativo non derivano oneri a carico dell'Azienda;

Disporre la notifica della presente deliberazione, unitamente al Regolamento in argomento, alle UU.OO. interessate e ai professionisti sanitari cui è rivolto;

Autorizzare la pubblicazione del Regolamento nella sezione dedicata del sito web Aziendale;

Munire la presente deliberazione della clausola di esecutività immediata, al fine di poter procedere ai successivi adempimenti.

Allegato: Regolamento sulla videosorveglianza e sull'uso dei dispositivi indossabili (c.d. bodycam) (parte integrante e sostanziale).

Il Direttore Amministrativo
(Dott. Carmelo Fabio Antonio Ferrara)



IL DIRETTORE GENERALE

Preso atto della proposta di deliberazione, che qui si intende riportata e trascritta, quale parte integrante e sostanziale del presente provvedimento;

Preso atto della attestazione di legittimità e di conformità alla normativa disciplinante la materia espressa dal Direttore Amministrativo che propone la presente deliberazione;

Sentito il parere favorevole del Direttore Sanitario;

D E L I B E R A

di approvare la superiore proposta, per come formulata dal Direttore Amministrativo e, pertanto, di:

Approvare e adottare il Regolamento Aziendale sulla videosorveglianza e sull'uso dei dispositivi indossabili (c.d. bodycam) (Allegato 1);

Dare atto che dal presente atto deliberativo non derivano oneri a carico dell'Azienda;

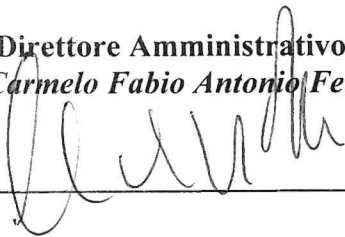
Disporre la notifica della presente deliberazione, unitamente al Regolamento in argomento, alle UU.OO. interessate e ai professionisti sanitari cui è rivolto;

Autorizzare la pubblicazione del Regolamento nella sezione dedicata del sito web Aziendale.

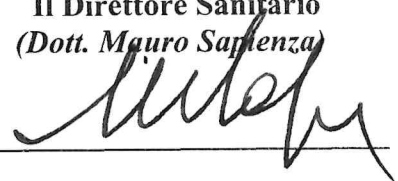
Munire la presente deliberazione della clausola di esecutività immediata, al fine di poter procedere ai successivi adempimenti.

ALLEGATO: Regolamento sulla videosorveglianza e sull'uso dei dispositivi indossabili (c.d. bodycam) (parte integrante e sostanziale).

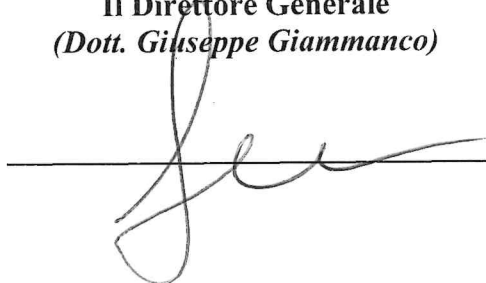
Il Direttore Amministrativo
(Dott. Carmelo Fabio Antonio Ferrara)



Il Direttore Sanitario
(Dott. Mauro Saplenza)



Il Direttore Generale
(Dott. Giuseppe Giammanco)



Il Segretario

Dott.ssa Antonella Cinardo



Copia della presente deliberazione è stata pubblicata all'Albo dell'Azienda il giorno

_____ e ritirata il giorno _____

L'addetto alla pubblicazione

Si attesta che la presente deliberazione è stata pubblicata all'Albo dell'Azienda dal _____

al _____ - ai sensi dell'art.65 l.r. n.25/93, così come sostituito dall'art.53 l.r. n.30/93-e

contro la stessa non è stata prodotta opposizione.

Catania _____

Il Direttore Amministrativo

Inviata all'Assessorato Regionale della Salute il _____ Prot. n. _____

Notificata al Collegio Sindacale il _____ Prot. n. _____

La presente deliberazione è esecutiva:

☒ immediatamente

☐ perché sono decorsi 10 giorni dalla data di pubblicazione

☐ a seguito del controllo preventivo effettuato dall'Assessorato Regionale per la Sanità:

a. nota di approvazione prot. n. _____ del _____

b. per decorrenza del termine

IL FUNZIONARIO RESPONSABILE

Azienda Ospedaliera di Rilievo Nazionale e di Alta Specializzazione "Garibaldi"

CATANIA

REGOLAMENTO VIDEOSORVEGLIANZA

Versione 00 del ____

Sommario

TITOLO I – Normativa e Definizioni.....	4
ART. 1 Normativa di Riferimento	4
ART. 2 Definizioni Specifiche	5
TITOLO II – Principi.....	5
ART.3 Principi Generali.....	5
ART. 4 Principio di liceità e correttezza.....	5
ART. 5 Principio di trasparenza	6
ART. 6 Principio di limitazione della finalità.....	6
ART. 7 Principio di minimizzazione dei dati	7
ART. 8 Principio di proporzionalità	7
ART. 9 Principio di integrità e riservatezza.....	8
TITOLO III – Soggetti.....	8
ART.10 Titolare.....	8
ART.11 Responsabile Protezione Dati	8
ART.12 Autorizzati	9
ART.13 Responsabile del Trattamento.....	9
TITOLO IV – Modalità	10
ART. 14 Risoluzione angolatura e panoramica delle riprese	10
ART. 15 Informativa e cartelli.....	10
ART. 16 Tipologia di ripresa	11
ART. 16 Videosorveglianza senza registrazione (Videocontrollo).....	11

ART. 17 Videocitofoni	12
ART. 18 Videosorveglianza con registrazione delle immagini	12
ART. 19 Utilizzo di dispositivi indossabili (c.d. bodycam)	13
TITOLO V – Misure di sicurezza e gestione dei supporti	14
ART. 20 Conservazione/Consegna della registrazione	14
ART. 21 Centrali di videocontrollo e/o Videosorveglianza – Accesso	15
TITOLO VI – Disciplina su settori specifici	16
ART. 22 Luoghi di lavoro	16
ART. 23 Luoghi di lavoro	18
TITOLO VII – Diritti degli interessati	19
ART. 24 Diritti degli interessati	19
TITOLO VIII – Installazione dei nuovi sistemi	20
ART. 25 Modalità di richiesta di nuovi sistemi di videosorveglianza/videoripresa	20
ART. 26 Partecipazione sindacale	22
ART. 27 Inosservanze e sanzioni	21
ART. 28 Disposizioni finali	22
Allegato 1 Modello semplificato Informativa Videosorveglianza senza registrazione (Videocontrollo)	
Allegato 2 Modello semplificato Informativa Videosorveglianza con registrazione	
Allegato 3 Modello semplificato Informativa Videosorveglianza con registrazione e collegamento alle Forze dell'Ordine	
Allegato 4 Informativa generale	
Allegato 5 Modello richiesta installazione nuovo impianto	
Allegato 6 Informativa Sul Trattamento delle immagini acquisite mediante Bodycam	
Addendum - modalità uso di bodycam	

TITOLO I – Normativa e Definizioni

ART. 1

Normativa di Riferimento

- **Codice Penale** articoli dal 318 a 322;
- **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”;
- **D.Lgs 30/06/2003 n. 196** “Codice in materia di protezione dei dati personali”, come da ultimo modificato dal **D. Lgs 101/2018**;
- **Provvedimento del Garante** per la Protezione dei dati personali adottato il 08/04/2010 “Provvedimento Generale sulla Videosorveglianza” (G.U. n. 99 del 29.04.2010);
- **Legge 10 dicembre 2014, n. 183** “Deleghe al Governo in materia di riforma degli ammortizzatori sociali, dei servizi per il lavoro e delle politiche attive, nonché in materia di riordino della disciplina dei rapporti di lavoro e dell'attività ispettiva e di tutela e conciliazione delle esigenze di cura, di vita e di lavoro”;
- **D.Lgs. 14 settembre 2015, n. 151** “Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183”;
- **D.Lgs. 24 settembre 2016, n. 185** “Disposizioni integrative e correttive dei decreti legislativi 15 giugno 2015, n. 81 e 14 settembre 2015, nn. 148, 149, 150 e 151, a norma dell'articolo 1, comma 13, della legge 10 dicembre 2014, n. 183”;
- **Regolamento UE 2016/679 del 27.04.2016** “Regolamento Generale sulla Protezione dei dati (di seguito Regolamento);
- **Nota Ispettorato del Lavoro** n. 299 del 28 novembre 2017
- **Circolare Ispettorato Nazionale del Lavoro (INL) n. 5 del 19 febbraio 2018**, avente ad oggetto “indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della legge n. 300/1970.”;
- **Delibere e provvedimenti aziendali** in materia di privacy.

ART. 2

Definizioni Specifiche

Videocontrollo: sistema o dispositivo che permette la visione unicamente in tempo reale di aree o zone delimitate;

Videosorveglianza: sistema o dispositivo che permette la visione e la registrazione su supporti singoli, abbinati ad altre fonti o conservati in banche di dati di immagini di aree o zone delimitate;

Videocitofoni: sistema o dispositivo installato in corrispondenza di campanelli o citofoni per finalità di controllo dei visitatori che si accingono ad entrare;

Centrale di Video controllo: sistema centrale dove sono convogliate ed eventualmente registrate tutte le riprese effettuate dai dispositivi periferici.

TITOLO II – Principi

ART.3

Principi Generali

1. Il trattamento dei dati personali derivante dall'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento civile e penale applicabili, comprese le vigenti norme in materia di controllo a distanza dei lavoratori (cfr. art.114 del D.Lgs. 196/2003 e ss.mm.ii., art. 4 Legge n. 300/1970, come modificato dai D.Lgs nn. 151/2015 e n. 185/2016);
2. l'ARNAS Garibaldi si impegna a garantire un livello elevato di tutela dei diritti e delle libertà fondamentali nonché della dignità degli interessati rispetto al trattamento dei dati personali effettuato mediante l'utilizzo di sistemi di videosorveglianza.

ART. 4

Principio di liceità e correttezza

1. Il trattamento dei dati personali (immagini), attraverso sistemi di videosorveglianza e/o di videocontrollo, è effettuato ricorrendo almeno una delle condizioni di liceità indicate dal

Regolamento UE (artt. 6 e 9) ed avviene nel rispetto di tutte le vigenti normative di cui al precedente articolo 3.

2. L'ARNAS Garibaldi effettua il trattamento per scopi determinati ed espliciti:
 - a. per il perseguimento delle proprie funzioni istituzionali riguardanti finalità di diagnosi, assistenza e terapia sanitaria (es. reparti di rianimazione, salute mentale, etc);
 - b. per il perseguimento di un legittimo interesse, costituito da
 - i. miglioramento della sicurezza delle persone all'interno degli ambienti di lavoro;
 - ii. tutela del patrimonio aziendale pubblico (luoghi, beni).

ART. 5

Principio di trasparenza

1. L'ARNAS Garibaldi deve indicare in maniera trasparente le modalità con cui i dati sono raccolti ed utilizzati. Tali informazioni devono essere facilmente accessibili e comprensibili.
2. L'informativa è fornita, agli interessati utilizzando:
 - a. il modello semplificato di informativa "minima" predisposto dal Garante per la Protezione dei dati personali (finalizzato a segnalare in maniera immediata l'esistenza dell'impianto di videosorveglianza, con registrazione o meno delle immagini, la finalità e il titolare);
 - b. un'informativa completa, cui è previsto il rinvio, (contenente tutte le informazioni di cui all'art. 13 del Regolamento).
3. L'informativa deve essere visibile da parte degli interessati e facilmente conoscibile. Per un dettaglio si rinvia al successivo articolo 15 del presente regolamento e agli allegati 1, 2, 3 e 4.

ART. 6

Principio di limitazione della finalità

1. L'ARNAS Garibaldi utilizza i dati per le specifiche finalità indicate nell'art. 4. Le finalità perseguite sono comunicate dal Titolare del trattamento nella specifica informativa relativa al trattamento dei dati (immagini) di impianti di videosorveglianza e/o videocontrollo (v. art. 15);
2. le aree aziendali che, generalmente, possono essere sottoposte a controllo video sono:

- a. Aree di degenza critica in cui è necessario che il personale sanitario tenga sotto controllo video i pazienti per la loro tutela in quanto non direttamente visibili dalle postazioni di lavoro;
- b. Aree perimetrali per fini di tutela del patrimonio;
- c. Aree e punti strategici per l'azienda (quali ad esempio: archivi di documentazione cartacea od iconografica, laboratori, ecc.);
- d. Aree con la finalità di tutela dell'utenza e degli operatori da possibili aggressioni, furti, rapine, danneggiamenti e atti vandalici;
- e. Aree di snodo e di elevata affluenza dell'utenza (ad esempio zona pronto soccorso, ecc.) per rilevare eventuali situazioni di pericolo a protezione delle persone, della proprietà e del patrimonio aziendale;
- f. Aree in cui si vuole rilevare situazioni di pericolo, sempre nel rispetto della L. 300/70 (ad es. locali di irraggiamento sacche, locali di congelamento, laboratori di tossicologia, ecc ...).

ART. 7

Principio di minimizzazione dei dati

1. Il trattamento dei dati attraverso sistemi di videosorveglianza e/o video controllo è effettuato riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, curando la scelta ed il posizionamento delle telecamere e dei relativi con di ripresa.
2. Il sistema degli impianti di videosorveglianza e/o videocontrollo, conseguentemente, è conformato in modo da conservare le immagini, in modo sicuro, per il tempo minimo necessario (tre giorni) a perseguire la finalità dichiarata.
3. L'installazione delle videocamere nei luoghi di lavoro avviene previo accordo con le R.S.U. aziendali e le OO.SS. e, in assenza, previa autorizzazione dell'Ispettorato del Lavoro.

ART. 8

Principio di proporzionalità

1. L'installazione di un sistema di videosorveglianza e/o videocontrollo sarà proporzionata all'effettivo grado di rischio presente nell'area.
2. L'installazione di nuovi impianti avverrà attraverso le modalità previste dal successivo Titolo VIII.

3. Va limitata rigorosamente la “registrazione” quando è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini.

ART. 9

Principio di integrità e riservatezza

1. I dati vengono trattati adottando le misure tecniche ed organizzative che assicurino un adeguato livello di sicurezza. Tali misure devono essere idonee a proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita, distruzione o danno accidentale, al fine di garantire la massima tutela dei diritti degli interessati.
2. La sicurezza dei dati, in base ai concetti di privacy “by design” e “by default” introdotti dal Regolamento, diventa essa stessa un principio cardine del trattamento, dal momento che viene prevista dal Titolare sin dal momento della progettazione dei sistemi di videosorveglianza. Pertanto la scelta dei luoghi, della posizione delle telecamere, nonché della configurazione del software utilizzato, sono progettate, per singolo impianto, nel rispetto del massimo grado di sicurezza possibile.

TITOLO III – Soggetti

ART.10

Titolare

1. Il titolare del trattamento dati è l’ARNAS Garibaldi, nella persona del suo legale rappresentante pro tempore, il Direttore Generale.

ART.11

Responsabile Protezione Dati

1. Il Responsabile della Protezione dei dati è la persona designata dal Direttore Generale, ai sensi dell’art. 37 del Regolamento UE 2016/679, con delibera n. 1101 del 26.10.2023, nella figura del Dott. Davide Morales i cui dati di contatto sono presenti sul sito web aziendale.

ART.12

Autorizzati

1. Gli autorizzati al trattamento dei dati (immagini) relativi all'attività di videosorveglianza sono quelli di cui alla delibera n. 145 del 30/10/2018 nominati dal Titolare, ai sensi dell'art. 28 del Regolamento UE 2016/679. Sono soggetti che, con diversi livelli di abilitazione nel trattamento, per esperienza, capacità ed affidabilità, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
2. Per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
3. Gli stessi effettuano il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni in materia e delle proprie istruzioni.
4. Sono autorizzati al trattamento:
 - i Direttori/Responsabili delle strutture aziendali (ex Responsabili) nell'ambito delle quali insistono impianti di Videosorveglianza e/o Videocontrollo: sono tutti autorizzati al relativo trattamento dei dati con il massimo livello di abilitazione e/o i Direttori/Responsabili cui istituzionalmente afferisce il trattamento della videosorveglianza nella sua generalità;
 - le persone fisiche (ex incaricati) assegnate alla UO istituzionalmente competente al trattamento dei dati della videosorveglianza o alla struttura ove insiste l'impianto, secondo l'ambito del trattamento consentito (visione, registrazione, conservazione, comunicazione, distruzione, manutenzione ...);
 - eventuale/i Responsabile/i (esterno) e suoi autorizzati.
5. Le operazioni di trattamento possono essere effettuate solo dai suddetti autorizzati che operano sotto la diretta autorità del Titolare o del Responsabile Esterno o Loro Delegato, attenendosi alle istruzioni impartite, secondo il proprio profilo di autorizzazione, che indica il trattamento consentito.

ART.13

Responsabile del Trattamento

1. L'utilizzo di personale esterno per la gestione e/o la manutenzione dei sistemi di Videosorveglianza e/o Videocontrollo segue le norme relative alla nomina quali Responsabili (esterni) del trattamento,

di cui all'art 28 del Regolamento UE 2016/679. Con lo stesso sarà sottoscritto apposito Accordo di Nomina a Responsabile Esterno, che disciplinerà le modalità di trattamento.

2. Il manutentore e/o il gestore dell'impianto di video sorveglianza e di videocontrollo dovrà produrre e consegnare all'Azienda un documento che descriva l'intervento effettuato che ne attesti la conformità alle vigenti regole in materia di privacy.

TITOLO IV – Modalità

ART. 14

Risoluzione angolatura e panoramica delle riprese

1. L'angolatura e la panoramica delle riprese deve essere effettuata con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere (spazi di esclusiva pertinenza zonale) evitando, dove possibile, aree comuni o antistanti abitazioni, anche nel rispetto delle indicazioni riportate nel citato Provvedimento del Garante del 2010.

ART. 15

Informativa e cartelli

1. Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona video sorvegliata e/o video controllata.
2. L'Azienda, a tal fine, adotta i modelli semplificati di informativa minima (cartelli), conformi a quelli previsti dall'Autorità Garante per la protezione dei dati personali nel citato provvedimento del 2010 – Allegati 1 2 e 3 – a seconda che l'impianto effettui o meno la registrazione, sia o meno collegato direttamente con le forze di polizia.
3. L'informativa deve essere collocata nelle immediate vicinanze dei luoghi ripresi, deve avere un formato ed una dimensione che ne permetta un'agevole leggibilità e un posizionamento tale da essere chiaramente visibile agli interessati.
4. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vengono installati più cartelli informativi.
5. Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
 - deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale;
 - può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate;
 - deve essere posto sia se la videosorveglianza presuppone una registrazione, sia se la videosorveglianza è solo a scopo di fruizione immediata;
 - deve contenere con il nome dell'Azienda e la finalità dell'attività di monitoraggio video.
6. Il testo della informativa completa è pubblicato sul sito web aziendale www.ao-garibaldi.ct.it nella sezione "privacy".
7. Gli autorizzati del trattamento dati rispondono del rispetto delle prescrizioni sopra riportate.

ART. 16

Tipologia di ripresa

La tipologia di videosorveglianza effettuata in Azienda si distingue in:

- Videosorveglianza senza registrazione di immagini (monitoraggi con sola visione delle immagini);
- Videosorveglianza con registrazione di immagini;
- Utilizzo di bodycam a tutela del personale sanitario.

ART. 16

Videosorveglianza senza registrazione (Videocontrollo)

1. L'installazione dei sistemi di video controllo è vietata nei casi in cui sia possibile adottare efficaci dispositivi di controllo alternativi (come la presenza di personale addetto alla vigilanza, ecc.), in considerazione del principio di proporzionalità.
2. La loro presenza deve essere segnalata attraverso una informativa agevolmente rilevabile con le caratteristiche previste da questo Regolamento (art. 15).
3. L'angolo di visuale e la panoramica delle riprese e l'informativa rispondono alle disposizioni del presente regolamento.

4. Nel modello semplificato di informativa minima, (Allegato 1) di cui al modello dell'Autorità Garante, va utilizzata la dizione "La **rilevazione**".

ART. 17

Videocitofoni

Si applicano all'installazione di Videocitofoni (anche collegati via web o rete locale) tutte le regole previste per il Videocontrollo.

ART. 18

Videosorveglianza con registrazione delle immagini

1. Si applicano all'installazione dei sistemi di Videosorveglianza tutte le regole previste per il Videocontrollo.
2. Nel modello semplificato di informativa minima (Allegato 2), di cui al modello dell'Autorità Garante, va utilizzata la dizione "La **registrazione**".
3. I sistemi di videosorveglianza possono eventualmente essere collegati direttamente con le Forze di Polizia, con o senza registrazione. In tal caso valgono le presenti regole ed, in particolare, il predetto collegamento deve essere noto agli interessati mediante il modello semplificato di informativa minimo di cui al modello dell'Autorità Garante del 2010 (Allegato 3).
4. In applicazione del principio di proporzionalità, la conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario a raggiungere la finalità perseguita.
5. Utilizzo di bodycam a tutela del personale sanitario.

ART. 19

Utilizzo di dispositivi mobili indossabili (c.d. bodycam)

1. In relazione al Decreto Legge 1 ottobre 2024 n. 137 come convertito con legge di conversione 18 novembre 2024 n. 171, recante "*Misure urgenti per contrastare i fenomeni di violenza nei confronti dei professionisti sanitari, socio-sanitari, ausiliari e di assistenza e cura nell'esercizio delle loro funzioni, nonché di danneggiamento dei beni destinati all'assistenza sanitaria*", questa ARNAS intende adottare sistemi di sicurezza a tutela del personale sanitario per la salvaguardia e la sicurezza personale dei lavoratori impegnati in attività di cure in situazioni di criticità e pericolo, nonché al fine di tutelare i beni dell'Azienda.
2. A tal fine, l'Azienda, in qualità di Titolare del Trattamento dei dati, intende dotare il personale dipendente di sistemi di microtelecamere (cd. Bodycam) che saranno indossate dal personale autorizzato e ben visibili all'utente/paziente, nel rispetto della normativa privacy di cui d.lgs. 30 giugno 2003, n° 196, recante il "*Codice in materia di protezione dei dati personali*", come modificato dal d.lgs. n. 101/2018 e dal Regolamento UE 2016/679, nonché del Provvedimento Generale sulla videosorveglianza emanato dal Garante Privacy in data 08.04.2010.
3. L'attivazione del sistema di bodycam deve essere oggetto di specifico accordo sindacale o di autorizzazione dell'Ispettorato del Lavoro. (Incontro del 23/01/2026 -13/02/2026)
4. L'utilizzo di tali sistemi di videoregistrazione (bodycam) è regolamentata da apposito "*addendum*" (cui si rinvia) che costituisce parte integrante del presente regolamento.
5. Le videocamere e le schede di memoria di cui sono dotati i sistemi di cui al comma precedente dovranno essere contraddistinte da un numero seriale che dovrà essere annotato in apposito registro recante il giorno, l'orario, i dati indicativi del servizio e la qualifica e nominativo del dipendente che firmerà la presa in carico e la restituzione. La scheda di memoria, all'atto della consegna ai singoli operatori, non dovrà contenere alcun dato archiviato. Il sistema di registrazione dovrà essere attivato solo in caso di effettiva necessità, ossia nel caso di insorgenza delle situazioni di pericolo scritte al comma 1.

TITOLO V – Misure di sicurezza e gestione dei supporti

ART. 20

Conservazione/Consegna della registrazione

1. La conservazione è limitata a poche ore, per un tempo non superiore alle 72 ore successive alla rilevazione.

- Qualora, ricorrano speciali esigenze di ulteriore conservazione dovute a:
- festività o chiusura degli uffici;
- adesione ad una specifica richiesta investigativa motivata dell'autorità giudiziaria o di polizia giudiziaria;
- esigenze tecniche o particolare rischio di attività svolta;
- evento documentato di aggressione fisica che abbia causato lesioni al personale
- (certificato da referto medico);
- - danneggiamento grave e documentato del patrimonio aziendale (verbale delle Forze dell'Ordine)

è ammesso un periodo di conservazione fino a sette giorni.

L'eventuale allungamento oltre i sette giorni è possibile **ESCLUSIVAMENTE**:

- a) Su richiesta formale dell'Autorità Giudiziaria o di Polizia Giudiziaria;
- b) Previa verifica preliminare del Garante Privacy, secondo la procedura di cui al Provvedimento n. 256/2017.

In tale ipotesi il Direttore/Responsabile richiedente deve produrre:

- documentazione oggettiva dell'evento (referto medico, verbale FdO, denuncia);
- motivazione specifica del rischio residuo;
- indicazione del termine preciso di conservazione richiesto (massimo 30 giorni).

Tale richiesta andrà indirizzata al Direttore Generale che unitamente al DPO Aziendale valuterà quanto rappresentato, attivando, in caso di positiva valutazione, le attività necessarie a rendere operativa tale richiesta.

2. I sistemi impiegati devono essere programmati 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.

In presenza di impianti basati su tecnologia non digitale o, comunque, non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di cancellazione dei dati registrati, detta operazione dovrà essere effettuata manualmente, nei tempi fissati.

3. I supporti non più utilizzati devono essere distrutti prima di essere cestinati.
 4. È facoltà del Titolare del trattamento dei dati consegnare immagini conservate a terzi aventi diritto *(in base agli scopi definiti nel presente regolamento)* riguardanti esclusivamente gli organi di polizia giudiziaria e magistratura, previo atto di richiesta scritta ufficiale in base alla procedura in allegato.
- Le operazioni materiali di estrazione ed esportazione delle immagini su supporto informatico sono eseguite esclusivamente dal personale autorizzato dell'Istituto di Vigilanza. È fatto assoluto divieto ai Reparti o al personale di inoltrare richieste dirette di estrazione alla UOS SIA, la quale non è autorizzata ad accedere ai contenuti registrati per tali finalità.

ART. 21

Centrali di videocontrollo e/o Videosorveglianza – Accesso

1. Le Centrali di Video controllo e/o Videosorveglianza sono posizionate in luoghi comunque controllati.
2. L'accesso a tali centrali deve essere sempre regolamentato e tracciabile.
3. I dispositivi di registrazione delle immagini devono essere protetti da serratura o da accesso autenticato.
4. Responsabile di tali adempimenti sono gli autorizzati al trattamento dei dati.
5. È possibile visionare da “remoto” sia le immagini in real time che quelle registrate, con le cautele previste dalla nota INL del 2017 nei casi in cui trattasi di installazione di impianti di allarme o antifurto dotati anche di videocamere o fotocamere che si attivano, automaticamente, in caso di intrusione da parte di terzi all'interno dei luoghi di lavoro. In particolare, l'accesso da postazione remota alle immagini in real time potrà essere autorizzato se debitamente motivato.
6. L'accesso alle immagini registrate, sia da remoto che “in loco” deve essere necessariamente tracciato anche tramite apposite funzionalità che consentano la conservazione dei “log di accesso” per un congruo periodo, non inferiore a sei mesi.

TITOLO VI – Disciplina su settori specifici

ART. 22 Luoghi di lavoro

1. La videosorveglianza è disciplinata dall'art. 4 della Legge n. 300/1970, successivamente modificato dal D.Lgs. n. 151/2015 e dal D. Lgs. n. 185/2016 come segue:

Art. 4 - Impianti audiovisivi. ⁽¹⁾

1. *Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi. ⁽²⁾*
2. *La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*
3. *Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.*

(1) Articolo così sostituito dall'art. 23, comma 1, D.Lgs. 14 settembre 2015, n. 151, a decorrere dal 24 settembre 2015, ai sensi di quanto disposto dall'art. 43, comma 1 del medesimo D.Lgs. n. 151/2015.

(2) Comma così modificato dall'art. 5, comma 2, D.Lgs. 24 settembre 2016, n. 185, a decorrere dall'8 ottobre 2016, ai sensi di quanto disposto dall'art. 6, comma 1, del medesimo D.Lgs. n. 185/2016.

2. Ai sensi dello stesso, L'ARNAS Garibaldi precisa che non effettuerà trattamenti di dati attraverso sistemi di videosorveglianza al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto degli orari di lavoro e la correttezza nell'esecuzione della prestazione lavorativa e non utilizzerà le immagini derivanti dagli impianti di videosorveglianza per controllo a distanza dei lavoratori. Tali immagini, ad esempio, non potranno essere utilizzate per un eventuale procedimento disciplinare.
3. L'attività di videocontrollo e/o videosorveglianza è ammessa solo ed esclusivamente per il perseguimento:
 - delle proprie funzioni istituzionali riguardanti il perseguimento di finalità di diagnosi, assistenza e terapia sanitaria;
 - del miglioramento della sicurezza delle persone all'interno degli ambienti di lavoro;
 - della tutela del patrimonio aziendale pubblico (luoghi, beni e persone).
4. L'installazione degli impianti dovrà essere concordata 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 (artt. 113 e 114 del Codice Privacy; art.38 n. 300/1970; art. 2 d.lgs n. 165/01). L'Accordo dovrà essere rinnovato ogniqualvolta ci sia un mutamento rispetto al precedente accordo siglato.
5. La ripresa diretta del lavoratore deve essere evitata per quanto possibile.
6. È inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (es. spogliatoi, bagni etc.).
7. Eventuali riprese televisive sui luoghi di lavoro per documentare attività o prestazioni solo per scopi divulgativi, scientifici o di comunicazione istituzionale, che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni di pensiero anche nell'espressione accademica, artistica e letteraria. In tal caso si applicano le disposizioni sull'attività giornalistica contenute nel Codice (art. 136) fermi restando i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico

per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine esercitando i diritti di cui al Capo III del Regolamento UE.

ART. 23

Luoghi di lavoro

1. Il controllo di ambienti sanitari ed il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad esempio UOC di rianimazione, UTIC, reparti di isolamento, etc), 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.
2. Considerata la natura sensibile dei dati, l'installazione e l'utilizzo degli impianti di ripresa nell'ambito di luoghi di cura dovrà garantire che il trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.
3. Il Titolare ed i Responsabili del trattamento devono garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (personale medico, infermieristico, tecnico etc).
4. Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conviventi, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione, UTIC etc), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente, previo specifico protocollo operativo, che sarà redatto dal Direttore/Responsabile della UO interessata e comunicato agli autorizzati al trattamento dei dati.
5. Al fine di garantire la necessaria riservatezza del paziente, i monitor riservati al controllo o destinati ai familiari devono essere posizionati in ambienti separati e normalmente non accessibili al pubblico.
6. Le riprese effettuate nell'ambito della psicoterapia sono soggette alla richiesta di consenso da parte del paziente (o tutore o esercente la patria potestà). Nel modulo di consenso deve essere specificamente riportata l'autorizzazione al trattamento dei dati tramite ripresa audiovisiva delle sedute.
7. Le riprese effettuate ai fini della formazione possono essere effettuate solamente previa autorizzazione del Titolare nonché informativa, consenso e liberatoria da parte degli interessati.

8. 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 malate su monitor collocati in locali liberamente accessibili al pubblico.

TITOLO VII – Diritti degli interessati

ART. 24 Diritti degli interessati

All'interessato è assicurato l'esercizio dei propri diritti, ai sensi della vigente normativa in materia di privacy e precisamente:

- diritto di accesso ai propri dati personali (art.15);
- diritto di cancellazione – cd. diritto all'oblio – (art. 17);
- diritto alla limitazione del trattamento (art. 18);
- diritto alla portabilità dei propri dati personali (art. 20);
- diritto di opposizione al trattamento dei dati personali (art.21)
- diritto di proporre reclamo all'autorità di controllo (art.13 c.2 lett. d).

Gli stessi potranno essere esercitati utilizzando l'apposita modulistica predisposta dall'Azienda e rinvenibile sul sito aziendale, secondo le seguenti modalità:

- a. l'interessato, previa verifica dell'identità ed entro le ventiquattro ore successive alla rilevazione, può richiedere per iscritto l'accesso alle registrazioni che lo riguardano.
L'eventuale accesso a registrazioni riferite direttamente o indirettamente a terzi sarà oggetto di apposita valutazione degli interessi da parte del Direttore/Responsabile della struttura interessata, autorizzato al trattamento dei dati.
- b. i dati sono estratti a cura degli autorizzati e possono essere comunicati direttamente al richiedente mediante la visione delle registrazioni e, se vi è richiesta, si provvede alla duplicazione di tali registrazioni su adeguato supporto fornito dal richiedente;
- c. la visione e l'estrazione delle rilevazioni è gratuita per l'interessato; qualora, tuttavia a seguito di questa operazione non risulti l'esistenza di dati che riguardano l'interessato potrà essergli addebitato un contributo spese, pari all'importo forfettario di € 50,00;

Per rispettare le scadenze entro la quale devono essere soddisfatte eventuali richieste, è ragionevole aspettarsi che il richiedente fornisca informazioni accurate per individuare i dati, indicando, ad esempio, un intervallo temporale preciso e il luogo/telecamera in cui sono state acquisite le riprese.

TITOLO VIII – Installazione dei nuovi sistemi

ART. 25

Modalità di richiesta di nuovi sistemi di videosorveglianza/videoripresa

1. L'attivazione di nuovi sistemi di videosorveglianza/videoripresa prevede il preliminare invio della richiesta al Direttore Generale (Modello 4) da parte del responsabile della struttura richiedente, riportante indicazioni circostanziate su:
 - a. motivazioni circa la necessità del sistema;
 - b. area da sorvegliare, orari di attivazione, eventuale presenza di personale dipendente e/o soggetti estranei nelle aree di ripresa;
 - c. evidenza sull'insufficienza di altri sistemi di controllo (ad es.: controllo accessi, sistemi di allarme, ecc.)
 - d. eventuale necessità di registrazione, finalità cui si ricollega la registrazione medesima, tempo di conservazione delle immagini e motivazioni per un eventuale tempo di conservazione superiore alle 72 ore;
 - e. eventuali caratteristiche tecniche delle apparecchiature;
2. La richiesta, contenente tutti gli elementi indicati dalla lett. a) alla lett. e), sarà inoltrata dal Direttore Generale ed al Responsabile Protezione dei Dati (DPO) che dovrà esprimere il parere unitario;
3. il Responsabile Protezione dei Dati (DPO), richiede pareri tecnici al Direttore dell'UOS S.I.A.
4. l'UOS SIA dovrà valutare, entro 15 giorni, la compatibilità dell'impiantistica richiesta con i sistemi e le reti esistenti, nonché la loro conformità tecnica alla normativa in materia di privacy e alle politiche in materia di sicurezza adottate dall'Azienda in materia, redigendo specifica relazione;
5. il Responsabile Protezione dei Dati (DPO), non appena l'UOS SIA avrà espresso il parere, per iscritto, con l'ausilio del gruppo di lavoro aziendale in materia di privacy, dovrà esprimere obbligatoriamente un parere unitario con eventuali proprie osservazioni predisponendo, altresì, la necessaria DPIA per valutare l'impatto del trattamento sulla protezione dei dati personali, ai sensi

dell'art. 35 del Regolamento UE 2016/679. Tale parere unitario, comprensivo dei documenti prodotti dall'UOS SIA e della DPIA effettuata, sarà inviato al Direttore Generale da parte del DPO.

6. Il Direttore Generale valuta la documentazione:
 - a. in caso di parere favorevole del DPO alla richiesta e suo parere concorde assume la DPIA e attiva, quindi, il successivo percorso di confronto con le OO.SS. e R.S.U, secondo le vigenti disposizioni di legge e di regolamento o, in caso di diniego, attiva la procedura con la sede territoriale dell'Ispettorato Nazionale del Lavoro;
 - b. in caso di parere favorevole del DPO alla richiesta e suo parere discorde esprime un parere negativo motivato. La procedura si interrompe con l'invio di tale parere a tutti gli attori coinvolti.
 - c. in caso di parere sfavorevole del DPO alla richiesta e suo parere concorde esprime un parere negativo. La procedura si interrompe con l'invio di tale parere a tutti gli attori coinvolti.
 - d. in caso di parere sfavorevole del DPO alla richiesta e suo parere discorde esprime un parere positivo motivato, proseguendo come al punto 6a.
7. Il Direttore Generale nei casi in cui prosegue nella procedura, siglato l'Accordo con le OO.SS./RSU aziendali o ottenuta l'autorizzazione dell'Ispettorato Provinciale del Lavoro invia il documento al DPO per gli adempimenti di competenza e per essere conservato agli atti.
8. Solo a completamento di tutto il procedimento sopra indicato il Direttore Generale invierà tutta la documentazione alla UO deputata all'acquisto, dandone contestuale comunicazione alle U.O.S. S.I.A.. Detta UO porrà in essere tutte le attività per acquisire il sistema di videosorveglianza.
9. Il Settore Tecnico Aziendale, in sinergia con la U.O.S. SIA per la sola parte di competenza networking e infrastrutturale, darà corso alle attività prodromiche all'acquisto e successive, compresa la progettazione esecutiva, la direzione lavori e il collaudo degli apparati..
10. Dopo il collaudo positivo, la gestione successiva (compresa la manutenzione ordinaria/straordinaria e l'estrazione delle immagini) è demandata all'Istituto di Vigilanza affidatario dell'appalto, formalmente nominato Responsabile Esterno del Trattamento (art. 28 GDPR). La competenza della UOS SIA è limitata esclusivamente al supporto infrastrutturale di rete.
11. Prima dell'attivazione del sistema l'UO deputata all'acquisto trasmette al DPO, e ad eventuali Organismi aziendali nominati, il documento di collaudo del sistema installato.

ART. 26

Partecipazione sindacale

1. Si dà atto che il presente regolamento verrà presentato alle organizzazioni sindacali rappresentative.
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. 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.

ART. 27

Inosservanze e sanzioni

La mancata osservanza del presente Regolamento comporta responsabilità disciplinare. In caso di violazione del presente regolamento e nei confronti di coloro che hanno posto in essere un comportamento non lecito, il Titolare del Trattamento provvederà a porre in essere tutte le azioni necessarie e le misure cautelative, previste in caso di inosservanza e comportamento illecito.

La rivelazione di informazioni ottenute attraverso il sistema di videosorveglianza, oltre a costituire violazione disciplinare, anche ai sensi del Codice di comportamento del personale dell'ARNAS, integra la fattispecie del reato di cui all'art. 326 del Codice Penale (Rivelazione ed utilizzazione di segreti d'ufficio), nonché le sanzioni previste dalla normativa in materia di privacy.

ART. 28

Disposizioni finali

1. Per tutto quanto non dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dal Regolamento UE 2016/679 e dal Codice in materia di protezione dei dati personali D.Lgs. 30 giugno 2003, n. 196 come da ultimo modificato dal D. Lgs 101/2018.
2. La disciplina contenuta nel presente regolamento e conseguentemente le intese sindacali in merito agli impianti di videosorveglianza sono vincolanti per tutti i lavoratori anche non iscritti alle Organizzazioni Sindacali firmatarie del presente accordo e dei lavoratori assunti successivamente alla data dello stesso.



3. Si dà atto che il presente regolamento verrà adeguato ogni qualvolta intervengano mutamenti significativi nell'organizzazione dell'Azienda o nell'impianto normativo.
4. Il presente regolamento verrà pubblicato all'interno del portale web dell'ARNAS Garibaldi

Allegato 1
Modello semplificato Informativa Videosorveglianza senza registrazione
(Videocontrollo)



Allegato 2
Modello semplificato Informativa Videosorveglianza con registrazione



Allegato 3

**Modello semplificato Informativa Videosorveglianza con registrazione e collegamento
alle Forze dell'Ordine**



Allegato 4

Informativa generale

ARNAS Garibaldi di Catania

Informativa per il trattamento dei dati personali per le attività di videosorveglianza

(Regolamento UE 2016/679 artt. 13 e 14)

L'ARNAS Garibaldi, a norma degli artt. 13 e 14 del Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito Regolamento), Le fornisce una serie di informazioni in ordine al trattamento dei suoi dati personali (immagini) di cui all'attività di videosorveglianza/videocontrollo, che può prevedere o meno la registrazione delle immagini.

TITOLARE DEL TRATTAMENTO DEI DATI è l'ARNAS Garibaldi di Catania, con sede legale in Piazza Santa Maria di Gesù n.5, 95124 Catania CT, nella persona del suo legale rappresentante pro-tempore il Direttore Generale.

Lo stesso potrà essere contattato tramite:

- posta ordinaria: all'indirizzo della sede legale dell'A.O.;
- e-mail: dir.generale@arnasgaribaldi.it;
- telefono: +39 095 7591 111;

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO), nominato ai sensi dell'art. 37 del Regolamento con provvedimento reperibile sul sito web del Titolare nell'apposita sezione Privacy, potrà essere contattato, per qualsiasi problematica riguardante la Sua privacy, ai seguenti recapiti:

- posta ordinaria: Responsabile Protezione Dati ARNAS Garibaldi – Piazza Santa Maria di Gesù n.5, 95124 Catania CT;
- e-mail: privacy@arnasgaribaldi.it
- pec: privacy@pec.ao-garibaldi.ct.it;

LE FINALITA' per le quali saranno trattati i dati (immagini) rilevate con la videosorveglianza:

- delle proprie funzioni istituzionali riguardanti il perseguimento di finalità di diagnosi, assistenza e terapia sanitaria;
- del miglioramento della sicurezza delle persone all'interno degli ambienti di lavoro;

- della tutela del patrimonio aziendale pubblico (luoghi, beni).

Si precisa che, qualora le telecamere siano posizionate per le finalità sopra indicate in ambienti di lavoro, le eventuali immagini che riprendano i lavoratori durante la loro prestazione di attività non potranno essere utilizzate per la finalità del controllo dei lavoratori

BASE GIURIDICA DEL TRATTAMENTO:

la base giuridica del trattamento dei suoi dati è costituita dal perseguimento dell'interesse legittimo del Titolare di tutela del patrimonio aziendale e sicurezza nei luoghi di lavoro e, quando installata nei luoghi di cura, dalla salvaguardia della salute dell'interessato.

DESTINATARI E CATEGORIE DI DESTINATARI DEI DATI PERSONALI:

Si informa che i Suoi dati potranno essere destinati ad altri soggetti e/o categorie di soggetti diversi quali: Autorità Giudiziaria in caso di richiesta, alla Ditta che effettua la manutenzione e/o gestione degli impianti.

PERIODO DI CONSERVAZIONE DEI DATI:

Le immagini saranno conservate per 72 ore successive alla rilevazione

Qualora, per speciali esigenze di ulteriore conservazione in relazione a:

- festività o chiusura degli uffici;
- adesione ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;
- esigenze tecniche o particolare rischiosità dell'attività svolta

sia necessario prevedere un tempo più ampio di conservazione dei dati, la conservazione non potrà comunque superare la settimana.

I DIRITTI

La informiamo dell'esistenza di alcuni diritti sui suoi dati personali e sul relativo trattamento che potranno essere esercitati:

- diritto di accesso ai propri dati personali (art.15)
- diritto di cancellazione – cd. diritto all'oblio – (art. 17);
- diritto alla limitazione del trattamento (art. 18);
- diritto alla portabilità dei propri dati personali (art. 20);
- diritto di opposizione al trattamento dei dati personali (art.21)
- diritto di proporre reclamo all'autorità di controllo (art.13 c.2 lett. d)

Per l'esercizio di tali diritti potrà utilizzare l'apposita modulistica predisposta dall'Azienda e rinvenibile sul sito web aziendale nell'apposita sezione privacy.

Allegato 5
Modello richiesta installazione nuovo impianto

Al Direttore Generale ARNAS Garibaldi
Piazza Santa Maria di Gesù n.5
95124 Catania CT

Oggetto: Richiesta acquisto e installazione nuovo impianto di videosorveglianza

Il sottoscritto Direttore Responsabile UO _____, atteso che presso _____ appare opportuno e necessario installare un nuovo impianto di videosorveglianza

inserire motivazioni circa la necessità dell'installazione del nuovo impianto

inserire le seguenti notizie:

1. area da sorvegliare:
2. orari di attivazione:
3. eventuale presenza di personale dipendente e/o soggetti estranei nelle aree di ripresa:

Evidenziare l'insufficienza di altri sistemi di controllo

specificare se è necessaria la motivazione della REGISTRAZIONE:

specificare la finalità cui si ricollega la registrazione medesima (*spuntare la finalità di interesse*):

- ☐ funzioni istituzionali riguardanti il perseguimento di finalità di diagnosi, assistenza e terapia sanitaria;
- ☐ miglioramento della sicurezza delle persone all'interno degli ambienti di lavoro;
- ☐ tutela del patrimonio aziendale pubblico (luoghi, beni).

indicare tempo di conservazione delle immagini e motivazioni per un eventuale tempo di conservazione superiore alle 72 ore;

specificare eventuali caratteristiche tecniche delle apparecchiature

Altro:

Si allega: (*eventuale*)

Il Direttore/Responsabile UO _____

Firma

PROTOCOLLO del DIRETTORE GENERALE

Si trasmette al Responsabile Protezione Dati (DPO), per il seguito di competenza

Data, _____

Il Direttore Generale

Firma

ALLEGATO 6
INFORMATIVA SUL TRATTAMENTO DELLE IMMAGINI ACQUISITE MEDIANTE
BODYCAM

in applicazione dell'art. 13 del REGOLAMENTO (UE) 2016/679 "GDPR"

Dati di contatto

Titolare del trattamento è l'Azienda Ospedaliera di Rilievo Nazionale e di Alta Specializzazione ARNAS "Garibaldi", nella persona del suo legale rappresentante pro-tempore il Direttore Generale, con sede in Piazza Santa Maria di Gesù n. 5 Catania - 95124, recapito telefonico 095 7591111, recapito di posta elettronica certificata protocollo.generale@pec.ao-garibaldi.ct.it e di posta elettronica privacy@arnasgaribaldi.it.

L'ARNAS Garibaldi ha provveduto alla nomina del Responsabile della Protezione dei Dati, che risponde al seguente riferimento: privacy@arnasgaribaldi.it.

Finalità del trattamento

Il trattamento dei dati mediante i dispositivi indossabili cd. body cam è finalizzato unicamente alla tutela della sicurezza degli operatori ospedalieri, prevenzione, repressione di atti criminosi e, in particolare, all'esigenze di sicurezza e incolumità delle persone e per le finalità di contrasto alle aggressioni al personale sanitario, nonché per la prevenzione e tutela del patrimonio aziendale. In particolare, le body cam sono utilizzate per prevenire ed impedire il compimento di fatti criminosi, consentendo di individuare i responsabili mediante registrazione degli stessi, acquisendo prove da utilizzare nel procedimento amministrativo relativo alla sanzione e/o nei procedimenti penali. Il trattamento dei dati raccolti mediante le body cam avverrà nel rispetto della disciplina di protezione dei dati personali e delle linee guida 3/2019 del Comitato europeo per la protezione dei dati (EDPB).

I dati trattati riguardano esclusivamente immagini riprese da telecamere portatili Body cam.

Base giuridica e liceità del trattamento

I Suoi dati personali (riprese video), raccolti attraverso le body cam, verranno trattati sulla base giuridica dell'interesse pubblico (art. 6 co. 1 lett. e) del GDPR, consistente nello svolgimento di attività di controllo e ispettive, nonché sanzionatorie e di tutela in sede amministrativa e/o giudiziaria.

Il trattamento è altresì basato sull'interesse legittimo volto alla tutela della sicurezza del personale e alla tutela del patrimonio aziendale del Titolare del trattamento, ai sensi dell'art. 6, par. 1, lett. f) del GDPR.

Modalità del trattamento

Ogni trattamento avviene mediante l'adozione di misure di sicurezza, tecniche ed organizzative, adeguate al trattamento stesso così come riportato all'art. 32 del GDPR. Tutti i dati sono trattati in forma elettronica e sono attuate misure idonee di minimizzazione del trattamento, quanto a tipologie del dato, autorizzazioni all'accesso e tempi di conservazione.

Si precisa che la videoripresa viene attivata solo allorché si verifichino situazioni tali da rendere possibile il prossimo verificarsi di fatti criminosi e/o illeciti.

Destinatari dei dati personali

Le immagini riprese sono registrate su supporto digitale e non saranno oggetto di diffusione. Il trattamento delle immagini è demandato esclusivamente a soggetti specificatamente autorizzati da ARNAS Garibaldi in conformità alle prescrizioni dettate in materia di sicurezza dei dati. Qualora espressamente richieste le immagini potranno essere fornite all'Autorità Giudiziaria, a membri delle Forze di Polizia e all'Istituto assicuratore per la tutela dei diritti, anche senza il consenso degli interessati. Tutti i destinatari dei dati sono comunque vincolati al rispetto della riservatezza.

Periodo di conservazione dei dati personali

I dati personali registrati saranno conservati per un lasso di tempo stabilito in 72 ore; nel caso in cui gli accadimenti video ripresi possano concretizzare fatti rilevanti penalmente e/o civilmente e/o sul piano amministrativo, solo le videoriprese che possono costituire fonte di prova saranno conservate sino alla definizione del procedimento.

Diritti dell'interessato

L'interessato gode dei diritti di cui all'art. 15 e ss. GDPR e precisamente i diritti di chiedere l'accesso ai dati che riguardano l'interessato, la loro cancellazione, la rettifica dei dati inesatti, l'integrazione dei dati incompleti, la limitazione del trattamento, la portabilità nonché l'opposizione al trattamento nelle ipotesi di legittimo interesse del Titolare. Le istanze di cancellazione e opposizione potranno essere accolte solo qualora non siano più sussistenti le



Azienda Ospedaliera
di rilievo nazionale e di alta specializzazione “GARIBALDI”
Catania

finalità di interesse pubblico. L’esercizio di tutti i diritti predetti potrà essere azionato in ogni momento scrivendo al Titolare del trattamento alla pec aziendale protocollo.generale@pec.ao-garibaldi.ct.it, oltreché contattando il Responsabile della Protezione dei Dati all’indirizzo privacy@arnasgaribaldi.it. Restano fermi i limiti previsti dagli artt. 23 GDPR, nonché 2-undecies e 2-duodecies Codice Privacy.

Ha il diritto di proporre reclamo all’Autorità di controllo competente nello Stato membro in cui risiede abitualmente o lavora o dello Stato in cui si è verificata la presunta violazione.

Processo decisionale automatizzato

I Suoi dati non saranno soggetti a processi decisionali automatizzati.

Addendum
al Regolamento
Videosorveglianza
**MODALITÀ USO DI
BODYCAM**

Obiettivi e Finalità:

Il presente atto costituisce un addendum al Regolamento della videosorveglianza dell'ARNAS Garibaldi e definisce le procedure e le modalità di utilizzo delle body cam in uso al personale dipendente. In particolare, l'uso delle body cam è finalizzato a prevenire e tutelare da minacce ed aggressioni la sicurezza e l'incolumità fisica degli operatori sanitari dell'Azienda Ospedaliera impegnati a svolgere le loro funzioni ed a tutelare il patrimonio dell'Azienda da danneggiamenti presso:

- il Pronto Soccorso;
- il Pronto Soccorso pediatrico;
- Pronto Soccorso Ostetricia e Ginecologia
- altre unità operativa in cui se ne ravvisi necessità.

Il trattamento dei dati raccolti mediante body cam si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale e per le sole finalità istituzionali dell'ARNAS Garibaldi. Le prescrizioni indicate nel presente documento vengono dettate in ottemperanza a quanto prescritto dalle seguenti fonti normative, nonché provvedimenti e pareri del Garante per la tutela dei dati personali:

- **Regolamento UE Generale sulla Protezione dei Dati 2016/679** 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”* (anche “RGPD/GDPR”);
- **Decreto Legislativo 30 giugno 2003, n. 196**, *“Codice in materia di protezione dei dati personali”* come modificato ed integrato dal D.Lgs 101/2018;
- **Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018**, pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018, inerente *“all'elenco delle tipologie di trattamenti, soggetti al requisito di una valutazione d'impatto*

sulla protezione dei dati ai sensi dell'art. 35 comma 4 del Regolamento UE n. 2016/679;

- **Direttiva UE 2016/680** relativa *“alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”*, recepita con il D.lgs. 51/2018;
- riferimento agli **articoli 7 del D.lgs. 51/2018** (sul trattamento di categorie particolari di dati personali),
- **Linee guida 03/2019 v.2 del 29 gennaio 2020 pubblicate dall'EDPB (European Data Protection Board)**, inerenti al trattamento di dati personali attraverso dispositivi video;
- **Provvedimento generale in materia di videosorveglianza in ambito pubblico e privato del 08 aprile 2010** del Garante della protezione dei dati personali (G.U. n. 99 del 29/04/2010);
- **Provvedimento Garante Privacy n. 362 del 22 maggio 2018** inerente alla *“Installazione di un sistema composto da bodycam per la raccolta e trasmissione di immagini riprese a bordo treno in tempo reale”*.
- **Parere Garante Privacy n. 290 del 22 luglio 2021** *“sulla valutazione di impatto del Ministero dell'Interno relativo ad un sistema di telecamere indossabili (body – cam), da parte dei Reparti mobili della Polizia di Stato, per la documentazione audio e video di situazioni critiche per l'ordine e la sicurezza, in occasione di eventi e manifestazioni pubbliche”*.

Per tutto quanto non risulti essere dettagliatamente disciplinato nel presente *addendum*, si fa rinvio alla normativa vigente in materia comunitaria e nazionale di protezione dei dati personali ed ai pareri dell' Autorità Garante Privacy.

Base giuridica del trattamento

Il trattamento dei dati personali effettuati tramite il sistema body cam può essere considerato lecito in quanto effettuato in ottemperanza alle disposizioni previste dall'art. 6 del Reg. UE 2016/679, ovvero per le seguenti finalità:

- per l'adempimento degli obblighi di sicurezza sui luoghi di lavoro di cui al D.Lgs. 81/2008 (art. 6.1. lettera c) GDPR);
- per l'esercizio di pubblici poteri (tutela della salute pubblica) (art. 6.1. lettera e) GDPR);
- per dati relativi alla salute eventualmente ripresi (art. 9.2. lettera b) GDPR);
- per la tutela del patrimonio aziendale (es. prevenire danneggiamenti) (Art. 6.1. lettera f) GDPR).

Nel caso in cui le Forze di Polizia o l'Autorità Giudiziaria richiedano la consegna di alcuni video per lo svolgimento delle indagini, la base giuridica del trattamento deve essere rinvenuta nell'adempimento ad un obbligo di legge a cui è soggetto il Titolare del trattamento, ai sensi dell'art. 6, par. 1, lett. c), del Reg. UE 2016/679.

Compatibilità dell'utilizzo delle bodycam con l'art. 4 della Legge n. 300/1970

L'utilizzo delle bodycam è subordinato al preventivo accordo sindacale o, in mancanza, all'autorizzazione dell'Ispettorato Territoriale del Lavoro, ai sensi dell'art. 4 della L. 300/1970.

Le immagini raccolte NON potranno essere utilizzate per:

- verificare l'adempimento della prestazione lavorativa;
- procedimenti disciplinari relativi all'attività lavorativa;
- controllo dell'orario di lavoro;
- valutazione delle performance del personale.

L'eventuale presenza di lavoratori nelle riprese è da considerarsi meramente incidentale rispetto alle finalità di sicurezza perseguite.

Necessità del trattamento

I dati personali raccolti devono essere adeguati, pertinenti e limitati a quanto necessari in relazione alle finalità per le quali sono trattati, nel rispetto di quanto previsto dal principio di " *minimizzazione dei dati* " dettato dall'art. 5, par. 1, lett. c) del Reg. UE 2016/679. Deve essere valutata l'eventuale sussistenza di altri mezzi meno invasivi dei diritti e delle libertà fondamentali dell'interessato rispetto all'utilizzo delle body cam e procedere alla loro attivazione solo nel caso si verifichi una potenziale fase di aggressione e/o minaccia nei confronti degli utenti e dipendenti dell'Azienda o il pericolo di danno ai beni di proprietà dell'Ente.

Modalità trattamento dei dati

L'utilizzo delle body cam è considerata una misura di "deterrenza", che viene utilizzata dall'Azienda quale attività di prevenzione del personale dipendente impegnato nell'attività di cura del paziente, avverso le minacce e/o aggressioni da parte del paziente o suoi accompagnatori o di pericolo in danno ai beni di proprietà dell'ARNAS. La modalità di trattamento dei dati dovrà pertanto avvenire come segue:

- a) La telecamera indossabile (bodycam), munita di scheda di registrazione, dovrà essere indossata dal dipendente e visibile all'utente;
- b) Le riprese audio e video dovranno, per quanto possibile, riprendere una visuale frontale, corrispondente allo specchio visivo dell'operatore e per quanto possibile non riprendere soggetti terzi. L'operatore dovrà segnalare all'utente l'attivazione del dispositivo.
- c) Gli operatori alla fine di ogni turno consegneranno la body cam al personale preposto dell'ARNAS. I dati video raccolti saranno estratti dal dispositivo tramite la formattazione della scheda di memoria e trasferiti su un apposito server aziendale a cui potranno aver accesso solo i soggetti autorizzati alla visione delle immagini;
- d) Al personale tenuto ad indossare il dispositivo sarà "preclusa la visualizzazione delle immagini registrate", essa sarà consentita solo al personale cui sono assegnati dal Titolare i compiti di visionare le immagini e di

segnalare/comunicare alle Autorità competenti i fatti criminosi.

e) Il personale autorizzato alla visione delle immagini sarà in possesso delle credenziali per accedere al sistema per la verifica delle immagini e la successiva trasmissione alle autorità competenti;

I dati verranno trattati da personale dell'ARNAS autorizzato ex art 2, *quaterdecies*, D. Lgs 196/2003 ed adeguatamente formato in materia di protezione dei dati personali ovvero da personale appositamente nominato ex art. 28 GDPR.

Procedura di gestione delle bodycam

1. CONSEGNA E REGISTRAZIONE

Le bodycam sono custodite in armadio blindato presso [specificare UO].

La consegna avviene tramite "Registro consegna/restituzione bodycam" che deve riportare:

- Data e ora di consegna;
- Numero seriale dispositivo e scheda memoria;
- Nome, cognome e matricola dell'operatore;
- Turno di servizio;
- Firma dell'operatore per presa in carico.

Prima della consegna, il Responsabile verifica che la scheda memoria sia formattata e vuota.

2. UTILIZZO

L'operatore indossa la bodycam in modo visibile sulla spalla/petto.

L'operatore procederà all'attivazione SOLO in caso di:

- Comportamento aggressivo manifesto dell'utente/accompagnatore;
- Minacce verbali gravi e reiterate;
- Tentativo di danneggiamento di beni aziendali.

Al momento dell'attivazione, l'operatore dichiara ad alta voce: "Sto attivando la registrazione video per ragioni di sicurezza".

L'operatore annota su apposito modulo (Allegato X):

- Ora di attivazione;
- motivo dell'attivazione;
- durata approssimativa della registrazione.

3. RESTITUZIONE

A fine turno, l'operatore riconsegna la bodycam.

Il personale incaricato dell'Istituto di Vigilanza verifica l'integrità del dispositivo e procede alla registrazione nel registro di ora di restituzione e firma.

Il personale incaricato dell'Istituto di Vigilanza trasferisce i dati dalla scheda al server aziendale entro 2 ore dalla restituzione.

Dopo il trasferimento verificato, la scheda viene formattata.

Le operazioni di trasferimento sono tracciate nel log di sistema.

4. SMARRIMENTO/DANNEGGIAMENTO DELLA BODYCAM

In caso di smarrimento, l'operatore redige immediata dichiarazione scritta.

L'operatore è responsabile dei danni cagionati alla bodycam che gli viene consegnata, a meno che non provi che il danno è causato da caso fortuito/forza maggiore (art. 2051 c.c.).

Viene attivata procedura di data breach ai sensi dell'art. 33 GDPR (notifica al Garante entro 72 ore se vi è alto rischio per i diritti e le libertà degli interessati).

Raccolta e Periodo di conservazione e obbligo di cancellazione

Il trattamento dei dati personali raccolti mediante l'uso delle *body cam*, avviene mediante registrazione video in maniera continuativa dal momento dell'accensione del dispositivo da parte del personale in movimento e si interrompe al momento della sua disattivazione.

Le immagini registrate vengono conservate dal Titolare del Trattamento per il tempo necessario all'effettiva verifica di eventuali minacce ed aggressioni/danni/ sottrazioni/ infrazioni/ intrusioni e comunque non oltre il tempo massimo di 72 ore, salvo specifiche richieste dell'autorità di polizia o giudiziaria; nel caso in cui i video abbiano ad oggetto eventi quali, a titolo esemplificativo: aggressioni, risse e danneggiamenti, il periodo di conservazione sarà di 5 anni, pari al termine di prescrizione ex art. 2947, comma 1 c.c., salvo che il fatto costituisca reato, per il quale è previsto un termine di prescrizione più lungo.

Obblighi di trasparenza e informazioni agli interessati

Ai sensi dell'art. 13 del Reg. UE 2016/679, il titolare del trattamento deve fornire agli interessati dettagliate informazioni in merito al trattamento dei dati effettuato. Alla luce delle situazioni in movimento e del volume di informazioni che è necessario fornire all'interessato, è preferibile seguire un approccio a diversi livelli:

- Informativa immediatamente visualizzabile resa con apposita cartellonistica posta nelle aree di ingresso alle stanze dove viene fornita assistenza sanitaria ai pazienti. Tale informativa potrà essere resa anche mediante

un'icona (QRcode) al fine di fornire, in modo facilmente visibile, comprensibile e chiaramente leggibile, una panoramica significativa del trattamento previsto.

- L'informativa completa reperibile presso la sede aziendale e pubblicata sul sito istituzionale dell'ARNAS Garibaldi che deve contenere tutti gli elementi previsti dall'art. 13 del Reg. UE 2016/679.

Infine, tenuto conto del fatto che le riprese potrebbero, seppur in via esclusivamente incidentale, riguardare i dipendenti e collaboratori, il titolare deve mettere a disposizione del personale una copia del presente addendum ed una copia dell'informativa sul trattamento dei propri dati personali, consultabili in qualunque momento anche mediante estrazione di copia.

Nel rispetto di quanto previsto dall'art. 4, comma 1, della legge 20 maggio 1970 n. 300, prima ancora di procedere all'utilizzazione del sistema body cam dal quale possa derivare la possibilità di controllo dei dipendenti, il Titolare deve siglare un accordo con le rappresentanze sindacali per l'utilizzo del sistema (nel caso in cui superi la soglia occupazionale di 15 dipendenti) oppure richiedere l'Autorizzazione all'installazione alla Direzione Territoriale del Lavoro (nel caso in cui la soglia occupazionale non venga superata).

Misure di sicurezza per la protezione dei dati

Come indicato nell'art. 25 del Reg. EU 2016/679, il Titolare del trattamento deve attuare misure tecniche e organizzative adeguate alla protezione dei dati raccolti mediante l'uso delle body cam, prima di iniziare la raccolta e il trattamento dei filmati video, tramite:

1. Misure di sicurezza organizzative, che definiscano con precisione i ruoli, le responsabilità connesse al sistema di raccolta delle immagini ed alla potenziale visualizzazione delle immagini;
2. Misure di sicurezza tecniche, per la protezione di tutti i componenti del sistema di raccolta delle immagini in tutte le fasi, vale a dire durante la memorizzazione, la trasmissione e l'elaborazione (visione).

Persone autorizzate al trattamento

Ai sensi dell'art. 2-quaterdecies del D. Lgs. 196/2003, così come modificato dal D.Lgs. 101/2018 e del Reg. UE 2016/679, il titolare del trattamento deve individuare formalmente i soggetti che, all'interno dell'ARNAS, siano autorizzati a raccogliere e ad accedere ai dati raccolti attraverso il sistema di body cam e, di conseguenza, a visualizzare le immagini nei casi in cui sia necessario per perseguire le finalità. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a raccogliere le immagini da coloro che possono visionare le immagini e successivamente comunicarle a terzi (autorità pubbliche o privati interessati).

LIVELLO 1 - UTILIZZO BODYCAM (personale operativo PS)

Autorizzati: Medici, infermieri, OSS in servizio presso PS/PS Pediatrico/PS Ostetrico

Operazioni consentite:

- Ritiro bodycam a inizio turno;
- Attivazione/disattivazione registrazione;
- Custodia durante il turno;
- Riconsegna a fine turno;

Operazioni VIETATE:

- Visione delle registrazioni;
- Estrazione dati dalla scheda;
- Cancellazione selettiva di registrazioni.

LIVELLO 2 - ESTRAZIONE DATI

Autorizzati: Personale incaricato dell'Istituto di Vigilanza (Responsabile Esterno). La UOS SIA si limita a garantire l'accessibilità e la sicurezza dell'infrastruttura server di destinazione.

Operazioni consentite:

- Trasferimento dati da scheda a server;
- Verifica integrità tecnica delle registrazioni;
- Formattazione schede dopo trasferimento;

Operazioni VIETATE:

- Visione del contenuto delle registrazioni;
- Comunicazione a terzi.

LIVELLO 3 - VISIONE IMMAGINI

Autorizzati:

- Responsabile Sicurezza [specificare nome/funzione]
- Direttore UOC Pronto Soccorso;
- n. 1 referente privacy designato

Operazioni consentite:

- Accesso alle registrazioni tramite credenziali personali;
- Visione per verificare eventi di aggressione/danno;
- Estrazione copie per Autorità (previa autorizzazione DG)

Operazioni VIETATE:

- Diffusione a soggetti non autorizzati;

- Utilizzo per finalità diverse da quelle dichiarate;

Tutte le operazioni di LIVELLO 3 sono tracciate in log conservati per 12 mesi.

Tali soggetti, il cui numero deve essere limitato a quanto strettamente necessario, devono essere nominati per iscritto e devono ricevere tutte le istruzioni in merito al corretto utilizzo del sistema. Tali istruzioni vengono fornite dal titolare e/o dal fornitore del sistema body cam.

In particolare, i soggetti autorizzati, impegnati nell'attività di cura dei pazienti potranno attivare le body cam solo in presenza di minacce, aggressioni o atti in danno ai beni aziendali.

Al personale tenuto ad indossare il dispositivo è “preclusa la visualizzazione delle immagini registrate”. Essi potranno accedere successivamente alle immagini per difendere i propri diritti dinnanzi alle Autorità competenti.

Le persone autorizzate al trattamento dei dati, visione delle immagini per verificare “i fatti”, potranno operare ed accedere alle stesse solo dalle apposite postazioni di controllo ed esclusivamente per gli scopi perseguiti, con l'obbligo di prestare la massima attenzione al fine di evitare che altri soggetti, anche inavvertitamente, possano prendere visione delle predette immagini secondo le seguenti procedure:

- Il monitor dal quale sia possibile visualizzare le immagini deve sempre essere rivolto in modo tale da evitare che altri soggetti non autorizzati possano, volontariamente o meno, prendere visione delle immagini.
- Nessun soggetto non autorizzato al trattamento dei dati deve poter accedere alle aree di controllo. Nel caso in cui queste ultime non siano costantemente presidiate, il dipendente o collaboratore dovrà assicurarsi di mettere in stand-by il monitor e di chiudere a chiave la stanza nella quale sia posizionato il monitor.
- In nessun caso le immagini acquisite tramite il sistema body cam potranno essere utilizzate per scopi di natura personale né per scopi differenti da quelli per i quali i dati sono raccolti.
- Le registrazioni contenenti i dati personali potranno essere estratte solamente su autorizzazione del Titolare, in seguito a potenziali eventi “lesivi” (minacce, aggressioni, furti, danni) per essere trasmesse alle autorità competenti per le ragioni di giustizia o su richiesta delle Autorità per finalità di indagini di polizia o giudiziaria. Queste ultime dovranno necessariamente essere formalizzate in forma scritta e conservate, quale evidenza della necessità di accedere i dati.

Tutte le persone autorizzate al trattamento devono attenersi strettamente alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle stesse.

Tutte le operazioni devono essere documentate in apposito “Registro consegna/restituzione delle bodycam-immagini registrate”.

Il mancato rispetto delle predette istruzioni può comportare l'irrogazione di sanzioni disciplinari, oltre che responsabilità di natura civilistica.

FORMAZIONE DEL PERSONALE

Prima dell'avvio del sistema bodycam, tutto il personale deve ricevere una formazione specifica (minimo 4 ore) su:

- Normativa privacy applicabile (GDPR, Codice Privacy, L. 300/1970);
- Finalità e limiti d'uso delle bodycam;
- Procedure di attivazione e criteri di necessità/proporzionalità;
- Gestione della catena di custodia;
- Diritti degli interessati e modalità di risposta;
- Gestione incidenti e data breach;
- Casi pratici e simulazioni.

Occorre procedere ad una formazione aggiuntiva annuale (2 ore) di aggiornamento normativo e procedurale. La partecipazione è documentata e tracciata. Il personale firma dichiarazione di presa visione delle procedure.

Per il personale di LIVELLO 2 e 3 (autorizzati ad estrazione/visione) occorre procedere a:

- Test di verifica competenze con soglia minima 80% risposte corrette;
- Rinnovo autorizzazione subordinato a superamento test annuale;

Responsabili del trattamento

Nel caso in cui l'installazione e la successiva gestione del sistema body cam vengano effettuati da una società esterna, quest'ultima deve essere preliminarmente nominata Responsabile del trattamento ai sensi dell'art. 28 del Reg. UE 2016/679, in relazione all'ambito di trattamento definito. La predetta nomina, con valenza contrattuale, deve essere redatta in forma scritta e deve contenere le istruzioni in merito al corretto trattamento dei dati personali.

A seguito della sua sottoscrizione, il responsabile è tenuto al rispetto di tutti gli obblighi dettati dall'art. 28 del Reg. UE 2016/679, tra i quali mettere a disposizione del Titolare del trattamento le informazioni necessarie per dimostrare il rispetto degli obblighi normativi e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento.

Misure di sicurezza tecniche

I dati raccolti mediante sistemi body cam devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.

In base alle caratteristiche dei sistemi utilizzati, i soggetti autorizzati al trattamento o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi raccoglie, accede alle immagini o controlla i sistemi di ripresa (controllo dei log). Il controllo degli accessi garantisce infatti che solo le persone autorizzate possano accedere al sistema e ai dati, mentre viene impedito agli altri di farlo.

Nel caso in cui sia necessario effettuare interventi di manutenzione, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini.

REQUISITI TECNICI MINIMI OBBLIGATORI

A. DISPOSITIVI BODYCAM

- Crittografia hardware dei dati sulla scheda memoria (AES-256 minimo);
- Timestamp sincronizzato con server NTP aziendale (non modificabile);
- Marcatura indelebile di data/ora su ogni frame video;
- Watermark digitale per verificare autenticità delle registrazioni;
- Numerazione seriale univoca e immutabile di dispositivo e scheda;
- Impossibilità per l'operatore di cancellare registrazioni dal dispositivo;
- Indicatore luminoso/sonoro di registrazione in corso (non disattivabile)
- Autonomia batteria minima: 8 ore di utilizzo continuativo;
- Grado di protezione: minimo IP65 (resistente a urti e schizzi)

B. TRASMISSIONE DATI

- Trasferimento **ESCLUSIVAMENTE** via cavo USB su postazione dedicata (NO trasmissione wireless per evitare intercettazioni);
- Postazione di trasferimento: PC dedicato, non connesso a Internet, in locale ad accesso controllato
- Software di trasferimento che genera hash SHA-256 di ogni file (per verificare integrità)
- Log automatico di ogni operazione di trasferimento con:
 - Numero seriale bodycam e scheda;
 - Data/ora trasferimento;
 - Operatore che effettua il trasferimento (autenticazione con smart card);

- Lista file trasferiti con relativi hash;
- Esito operazione

C. ARCHIVIAZIONE

Server dedicato ESCLUSIVAMENTE alle registrazioni bodycam:

- Storage crittografato (LUKS o equivalente);
- Backup automatico giornaliero su sistema segregato;
- Sistema di cancellazione automatica dopo 72 ore (o termine autorizzato);
- Cancellazione sicura (overwrite multipli secondo standard NIST);
- Log di cancellazione con data/ora e lista file eliminati;
- Sistema RAID per ridondanza (minimo RAID 5);
- UPS per prevenire perdite dati da interruzioni elettriche

D. ACCESSO ALLE REGISTRAZIONI

Autenticazione forte a due fattori (smart card + PIN o biometria)

- Logging completo di ogni accesso:

- Utente che accede (identificazione univoca);
- Data/ora di inizio e fine sessione;
- File visualizzati;
- Operazioni effettuate (play, pausa, estrazione copia);
- Indirizzo IP della postazione;
- Postazione di visione in locale segregato, monitor non visibile dall'esterno;
- Impossibilità di estrazione dati su USB/dispositivi mobili (porte fisicamente disabilitate)

Estrazione copie SOLO tramite funzione dedicata che:

- Richiede motivazione scritta;
- Genera file con watermark identificativo;
- Traccia l'estrazione in log inviolabile

E. CONTROLLI E AUDIT

- Revisione mensile dei log di accesso da parte del DPO
- Verifica trimestrale integrità tecnica dei sistemi (penetration test limitato)

- Audit annuale completo del sistema bodycam
- Test semestrale procedura di cancellazione automatica
- Verifica annuale delle nomine e delle autorizzazioni.

MONITORAGGIO E AUDIT

CONTROLLI PERIODICI

Il sistema bodycam è soggetto ai seguenti controlli:

MENSILI:

- A cura della UOS SIA (lato server): Verifica funzionamento degli automatismi di cancellazione e verifica integrità dei backup.
- A cura del DPO e del Responsabile Sicurezza/Vigilanza: Analisi dei log di accesso alle registrazioni e controllo del registro cartaceo/digitale di consegna/restituzione bodycam."

TRIMESTRALI (a cura DPO):

- Campionamento registrazioni (max 5%) per verifica conformità uso;
- Interviste a operatori su difficoltà/criticità riscontrate;
- Verifica rispetto dei tempi di conservazione;
- Controllo completezza della documentazione (registro, motivazioni conservazione >72h);

SEMESTRALI (a cura DPO + audit interno):

- Test completo di Disaster Recovery
- Verifica validità nomine e autorizzazioni
- Controllo formazione personale (partecipazione e registri)
- Simulazione di data breach

ANNUALI (a cura audit interno/esterno):

- Audit completo del sistema
- Penetration test delle infrastrutture
- Revisione DPIA
- Verifica conformità a linee guida Garante/EDPB aggiornate
- Report al Direttore Generale con raccomandazioni

Tutti i controlli sono documentati e conservati per 5 anni.

Le non conformità rilevate devono essere risolte entro 30 giorni (se gravi) o 90 giorni (se minori).

DATA BREACH E DISASTER RECOVERY

- **Gestione incidenti e continuità**

A. DATA BREACH

In caso di violazione dei dati (es. smarrimento bodycam, accesso non autorizzato, esfiltrazione dati), si attiva la seguente procedura:

1. RILEVAZIONE (entro 1 ora dalla scoperta)

L'operatore/responsabile che rileva l'incidente ne dà immediata comunicazione a:

- Direttore Sanitario;
- DPO;
- Responsabile UOS SIA;
- Compilazione "Scheda segnalazione incidente" (Allegato Y)

2. CONTENIMENTO (entro 4 ore)

- Blocco immediato credenziali di accesso se compromesse;
- Isolamento del sistema se attacco informatico;
- Recupero dispositivo se possibile;
- Blocco della diffusione se violazione in corso.

3. VALUTAZIONE (entro 24 ore)

Il DPO, con supporto SIA, valuta:

- Tipologia e gravità della violazione;
- Numero di interessati coinvolti;
- Tipologia di dati compromessi (particolari/comuni);
- Rischio per diritti e libertà degli interessati;
- Decisione su notifica al Garante (art. 33 GDPR - 72 ore) e comunicazione agli interessati (art. 34 GDPR).

4. RIMEDIO E DOCUMENTAZIONE

- Implementazione misure correttive;

- Aggiornamento registro dei trattamenti;
- Redazione report finale dell'incidente;
- Valutazione esigenza di DPIA aggiornata.

B. DISASTER RECOVERY

- Backup giornaliero delle registrazioni non ancora scadute;
- Piano di ripristino con RTO (Recovery Time Objective) = 24 ore;
- Procedura di ripristino testata semestralmente;

In caso di guasto del server principale occorre procedere a:

- Attivazione server di backup entro 4 ore;
- Ripristino dati dal backup più recente;
- Verifica integrità delle registrazioni ripristinate (controllo hash).

DPIA (data protection impact assessment)

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

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

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

AGGIORNAMENTO DELLA DPIA

La valutazione d'impatto deve essere riesaminata e aggiornata nei seguenti casi:

- a) Almeno ogni 24 mesi dalla precedente valutazione;
- b) Estensione del sistema bodycam ad altre Unità Operative oltre a PS/PS Pediatrico/PS Ostetrico;
- c) Modifica sostanziale delle finalità di trattamento;
- d) Implementazione di nuove funzionalità (es. riconoscimento facciale, trasmissione dati in tempo reale);
- e) Cambio significativo del fornitore o della tecnologia utilizzata;
- f) Dopo ogni data breach rilevante;

g) Su richiesta motivata del DPO;

h) Su richiesta del Garante Privacy;

L'aggiornamento della DPIA deve essere completato entro 60 giorni dall'evento scatenante e trasmesso al Garante se comporta nuovi rischi elevati.

Diritti degli interessati

In relazione al trattamento dei dati personali, agli interessati identificabili deve essere assicurato l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento e di ottenere l'interruzione di un trattamento illecito. Ai potenziali interessati deve essere rilasciata idonea informativa ai sensi degli artt. 13 - 22 GDPR.

DIRITTO DI ACCESSO

A. RICHIESTE DI ACCESSO

Le richieste di accesso alle registrazioni da parte di Autorità giudiziaria e Forze dell'Ordine devono:

- Essere formulate per iscritto su carta intestata;
- indicare: l'autorità richiedente, il riferimento del procedimento, il periodo temporale, la motivazione;
- essere protocollate e conservate.

Il Titolare del trattamento, previo parere del DPO:

- Verifica la legittimità della richiesta;
- Predisporre risposta entro 15 giorni (salvo urgenze motivate);
- Autorizza l'Istituto di Vigilanza all'estrazione materiale di copia delle registrazioni richieste con watermark identificativo;
- Traccia l'operazione in apposito registro.

B. CONSEGNA SPONTANEA

In caso di grave aggressione con lesioni al personale, il Titolare può valutare la trasmissione spontanea delle registrazioni alla Procura della Repubblica:

- Previa denuncia/querela formale della vittima;
- previa valutazione del DPO sulla proporzionalità;
- con comunicazione formale che specifichi: evento, data, orario, soggetti coinvolti (se noti);
- conservando copia della registrazione trasmessa fino alla definizione del procedimento penale.

Ogni comunicazione a terzi (anche Autorità) è documentata e tracciata.