

# **Disciplinare interno per l'utilizzo della piattaforma bodycam e strumenti informatici annessi**

## Sommario

<b>1. INTRODUZIONE .....</b>	<b>4</b>
1.1 Finalità del documento .....	4
1.2 Contesto normativo .....	5
<b>2. GLOSSARIO E DEFINIZIONI .....</b>	<b>6</b>
<b>3. PRINCIPI GENERALI .....</b>	<b>8</b>
<b>4. REGOLE PER L'UTILIZZO DEL SISTEMA BODYCAM .....</b>	<b>9</b>
4.1 Credenziali di autenticazione all'applicazione.....	9
4.2 Utilizzo di applicazioni aziendali .....	10
4.3 Postazione di lavoro .....	10
4.4 Postazione di lavoro portatile .....	11
4.5 Altri dispositivi .....	11
4.6 Software a corredo .....	11
4.7 Navigazione in internet .....	12
4.8 Posta elettronica .....	12
4.9 Servizi di Unified Communication (chat, messaggistica, videoconferenza, telefonia) .....	13
4.10 Servizi Cloud e Spazi di condivisione di rete aziendale .....	13
4.11 Dispositivi di memorizzazione rimovibili (Hard disk, Pen drive USB, etc.) .....	13
4.12 Comportamenti non consentiti .....	14
4.13 Protezione contro furti e danneggiamenti .....	15
<b>5. CONTROLLI E MONITORAGGI.....</b>	<b>16</b>
5.1. Ruolo degli amministratori delle risorse tecnologiche condivise e delle applicazioni.....	16

<b>6. RESPONSABILITÀ E SANZIONI .....</b>	<b>18</b>
<b>7. PRIVACY E DATA PROTECTION .....</b>	<b>18</b>

## 1. INTRODUZIONE

L'Azienda Sanitaria Locale di Salerno, di seguito denominata ASL, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento definisce le regole e le condizioni per l'utilizzo degli **strumenti bodycam della ASL** da parte dei dipendenti e di tutti coloro che, in virtù di un rapporto di lavoro a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, etc.), utilizzano tali strumenti della ASL, nel seguito denominati Utenti.

Il presente disciplinare deve considerarsi parte integrante di tutte le procedure interne adottate in ASL, fra cui la procedura prevista in caso di violazione di dati personali.

### 1.1 Finalità del documento

Il presente documento definisce e detta agli Utenti specifiche regole e condizioni di utilizzo delle bodycam aziendali attraverso:

- definizione di regole e procedure uniformi da applicarsi in tutte le aree operative dove sono utilizzate le bodycam:
  - UOC Emergenza - COT 118 - Urgenza Territoriale, presso le sedi di 118;
  - UOSD Tutela Salute Adulti e Minori Area Penale, presso Direzione della UOSD di Via Generale Clark di Salerno, Casa Circondariale di Salerno, Casa di reclusione di Eboli, Casa Circondariale di Vallo della Lucania
  - UOSD Servizio Psichiatrico di Diagnosi e Cura comprensive delle aree di accesso ai Pronto Soccorso di riferimento, presso PO di Nocera (SPDC), PO di Vallo della Lucania (SPDC), AOU Ruggi D'Aragona di Salerno (SPDC).
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;

- definizione dell'ambito, delle modalità e dei limiti del monitoraggio e dei controlli attuabili dalla ASL nel rispetto della normativa vigente nonché delle regole e delle procedure interne;
- individuazione delle responsabilità degli Utenti in caso di inosservanza di regole e prescrizioni.

## **1.2 Contesto normativo**

Il presente disciplinare è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8;
- D. Lgs. 196/2003 e s.m.i (Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);
- D.P.R. 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento ASL;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)

## 2. GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- **Amministratori di sistema:** figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;
- **Applicazioni aziendali:**  
Si considerano applicazioni aziendali:
  - Prodotti/programma acquistati dall'amministrazione, di valenza generale o settoriale ed in quest'ultimo caso approvati dai sistemi informativi;
  - Applicazioni e servizio sviluppate ad hoc dai sistemi informativi, da terze parti ma sotto il coordinamento dei sistemi informativi ovvero da altre strutture con un processo di partecipazione e approvazione da parte dei sistemi informativi e che seguono le regole di gestione previste nei casi precedenti;
  - Applicazioni esterne che l'amministrazione utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.
- **Dispositivi mobili:** apparecchi di telecomunicazione portatili (bodycam, docking station, tablet, smartphone, etc.);
- **File di log:** registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
- **Pila software:** elenco di software installati o installabili sui dispositivi aziendali ASL;

- **Postazione di lavoro (PdL):** personal computer (desktop o portatile) messo a disposizione dalla ASL a ciascun Utente per l'espletamento dell'attività lavorativa;
- **Strumenti informatici:** personal computer fissi o portatili, bodycam o docking station, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
- **Utenti:** personale dipendente, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro in essere a qualsiasi titolo con la ASL, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione dalla ASL.

### **3. PRINCIPI GENERALI**

Gli strumenti informatici sono assegnati agli Utenti per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e mediante comportamenti adeguati ai compiti assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e delle normative e direttive interne.

Nell'esecuzione della propria attività lavorativa, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

- a) effettuare la propria attività uniformandosi alle disposizioni della ASL e alle istruzioni ricevute;
- b) custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
- c) mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
- d) in caso di cessazione dal servizio o dalla prestazione svolta per la ASL, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività;
- e) adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;
- f) garantire la corretta custodia di atti e documenti adottati dalla ASL.



## **4. REGOLE PER L'UTILIZZO DEL SISTEMA BODYCAM**

### **4.1 Credenziali di autenticazione all'applicazione**

L'accesso all'applicazione del sistema informativo fornito alla ASL avviene attraverso autenticazione mediante credenziali di dominio.

Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti.

In caso di diffusione accidentale, anche solo presunta, le password devono essere immediatamente modificate e l'incidente va immediatamente segnalato.

Il sistema di controllo degli accessi presente nella ASL implementa le seguenti regole:

- composizione di password complesse, che abbiano una lunghezza minima stabilita e una sequenza di caratteri normali, speciali e/o numerici;
- modifica della password al primo utilizzo;
- validità minima e massima della password;
- impossibilità di riuso delle ultime password utilizzate;
- blocco dell'utenza dopo un determinato numero di tentativi falliti di inserimento della password;
- reinizializzazione (reset) della password e riattivazione delle utenze disabilite, secondo le procedure in vigore.

I dettagli dei requisiti richiesti sull'utilizzo delle password sono riportati nelle indicazioni fornite dell'U.O.C. Servizio Informativo Aziendale.

Al fine di aumentare il livello di sicurezza, ASL ha scelto di implementare un sistema di Multi Factor Authentication (MFA), richiedendo all'Utente di dimostrare la propria identità attraverso più forme di verifica al momento dell'accesso a un'applicazione.

I dettagli delle modalità MFA sono riportate nelle indicazioni fornite dell'U.O.C. Servizio Informativo Aziendale.

## **4.2 Utilizzo di applicazioni aziendali**

L'accesso alle applicazioni aziendali e il loro utilizzo devono avvenire secondo le regole dettate dal presente Disciplinare, con riferimento ai diversi ruoli di responsabilità specificamente individuati in ASL per le varie tipologie di utenza con relative funzioni di utilizzo della piattaforma bodycam.

All'atto della cessazione/interruzione del rapporto di lavoro o dell'attività lavorativa svolta a qualsiasi titolo per conto della ASL, è fatto obbligo la disabilitazione all'uso della utenza parte dell'U.O.C. Servizio Informativo Aziendale e di conseguenza la cessazione dell'accesso all'applicativo utilizzato per l'esplicazione delle funzioni connesse al rapporto di lavoro.

In caso di assegnazione temporanea del personale ASL presso altra pubblica amministrazione, durante il relativo periodo di servizio, l'U.O.C. Servizio Informativo Aziendale deve provvedere alla disabilitazione all'uso dell'utenza, fermo restando l'obbligo del dipendente di restituzione della strumentazione bodycam eventualmente assegnata dalla ASL per lo svolgimento della prestazione lavorativa.

## **4.3 Postazione di lavoro**

Le postazioni di lavoro (PdL) sono gestite dalla ASL. È vietato qualsiasi utilizzo che deturpi o rovini la PdL e tutti gli accessori/periferiche in assegnazione.

La postazione di lavoro è provvista di software di sicurezza (software antivirus, personal firewall, software per aggiornamento automatico delle patch di sistema, etc.).

La PdL deve essere provvista del software base approvato dalla ASL, tra cui necessariamente per l'utilizzo del sistema bodycam, di un browser web.

L'Utente assegnatario della postazione di lavoro è responsabile del suo corretto utilizzo nel rispetto delle seguenti regole comportamentali:

- a) la PdL è assegnata all'Utente per lo svolgimento della propria attività lavorativa;
- b) la PdL non deve essere accessibile a soggetti non autorizzati;
- c) l'Utente non deve apportare modifiche alle configurazioni della PdL che non

siano state preventivamente richieste e autorizzate dall'U.O.C. Servizio Informativo Aziendale;

- d) durante l'allontanamento dalla PdL, l'Utente deve bloccare la propria postazione per consentirne l'accesso unicamente mediante l'immissione della password;
- e) al termine della giornata lavorativa, soprattutto per motivi di sicurezza, deve essere effettuato lo spegnimento delle PdL.

#### **4.4 Postazione di lavoro portatile**

Per quanto riguarda la postazione portatile, valgono tutte le regole già descritte per le postazioni fisse.

Si evidenzia che le stazioni di lavoro portatili, utilizzate al di fuori della ASL, sono maggiormente esposte a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute. Tutti gli Utenti, pertanto, devono custodire con cura e diligenza la postazione di lavoro portatile assegnata.

Le postazioni di lavoro portatili devono essere verificate dall'U.O.C. Servizio Informativo Aziendale per l'installazione di eventuali aggiornamenti e/o patch di sicurezza. In caso di significativo rischio di compromissione o/e sicurezza, tale Servizio può richiedere all'Utente lo spegnimento della PdL portatile fino a tale verifica.

#### **4.5 Altri dispositivi**

Con riferimento ad altri dispositivi assegnati ai dipendenti, quali smartphone e/o tablet, valgono le medesime regole comportamentali adottate per le PdL.

#### **4.6 Software a corredo**

Per l'utilizzo delle bodycam non viene fornito software aggiuntiva da installare sulle PdL rispetto a quanto già in uso.

#### **4.7 Navigazione in internet**

La navigazione in internet è messa a disposizione del personale per le finalità utili allo svolgimento della prestazione lavorativa.

Qualsiasi operazione effettuata sulla rete esterna (accesso a siti web per necessità non inerenti all'attività lavorativa, salvataggio di file, partecipazione a forum, etc.) è posta sotto la responsabilità dell'Utente, che deve mantenere un comportamento lecito e tale da non compromettere le attività e il buon nome della ASL e dell'applicativo bodycam.

Al fine di garantire il corretto funzionamento dell'applicativo bodycam, ogni Utente è tenuto a osservare le seguenti regole comportamentali:

- utilizzare internet per fini leciti, astenendosi da qualsiasi comportamento che possa avere natura oltraggiosa e/o discriminatoria verso terzi;
- trasferire sul proprio computer (download) solo file da siti web verificati e affidabili, tenendo presente che quando si trasferisce materiale da internet occorre prestare la massima attenzione;
- non utilizzare social network, forum, chat e simili per scambiare informazioni riservate o lesive dell'immagine della ASL, dei colleghi o del software bodycam in utilizzo;
- la navigazione in internet avviene in modalità trasparente e non anonima, soprattutto se attraverso intranet o strumenti aziendali; in ogni caso è vietato accedere a siti i cui contenuti non siano autorizzati dalla ASL e possano compromettere l'integrità della PdL e del browser web utilizzato per la connessione all'applicativo bodycam.

#### **4.8 Posta elettronica**

Tutti gli Utenti che hanno accesso alla visualizzazione dei filmati sono dotati di una casella di posta elettronica sul dominio della ASL. Le caselle devono essere utilizzate per l'esercizio della propria attività lavorativa.

Quando si utilizza lo strumento della posta elettronica, è opportuno osservare comportamenti consoni, come indicato dall'U.O.C. Servizio Informativo Aziendale.

Nell'utilizzo del servizio l'Utente non deve diffondere, per mezzo della posta elettronica, anche ad altri colleghi, i messaggi di posta elettronica ricevuti dall'applicativo bodycam.

Ulteriori dettagli sull'utilizzo della posta elettronica sono riportati nelle indicazioni fornite dall'U.O.C. Servizio Informativo Aziendale.

#### **4.9 Servizi di Unified Communication (chat, messaggistica, videoconferenza, telefonia)**

Gli strumenti di Unified Communication (UC), oltre alla posta elettronica, comprendono la chat, la telefonia, la videoconferenza e la collaborazione sui documenti. L'oggetto che transita nella UC è la comunicazione e valgono le medesime regole comportamentali adottate per le PdL. Gli Utenti vengono identificati con il proprio User Principal Name (UPN). Il sistema di UC prevede la possibilità di inviare messaggi, effettuare videoconferenze, telefonare e, previo consenso di tutti i partecipanti, registrare ognuna delle suddette comunicazioni. I partecipanti alla comunicazione hanno la responsabilità del proprio comportamento e del rispetto della netiquette, i partecipanti, inoltre, sono responsabili delle informazioni scambiate. Nessuna informazione deve essere scambiata relativamente anche se in maniera indiretta del sistema bodycam.

#### **4.10 Servizi Cloud e Spazi di condivisione di rete aziendale**

Gli **spazi di condivisione** file server (on premise) o cloud, che sono utilizzati per la memorizzazione di file anche ad uso strettamente lavorativo, non devono contenere file e o informazioni esportate dall'applicativo delle bodycam.

#### **4.11 Dispositivi di memorizzazione rimovibili (Hard disk, Pen drive USB, etc.)**

L'utilizzo di supporti di memorizzazione rimovibili deve essere effettuato con molta cautela ed esclusivamente per le attività lavorative.

L'utilizzo di dispositivi rimovibili, utile per le attività legate all'esportazione delle

evidenze audio/video ai fini giudiziari, rimane in ogni caso sotto la responsabilità dell'utilizzatore. È vietato consegnare a terzi supporti già utilizzati per la memorizzazione di informazioni o di dati personali, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo l'intervenuta cancellazione.

L'Utente è tenuto a informare immediatamente i dirigenti responsabili della struttura organizzativa di appartenenza e il Responsabile della Protezione dei Dati, anche ai sensi della procedura di gestione delle violazioni di dati personali, di qualsiasi danno, furto o perdita di apparati, software e/o dati in proprio possesso che contengono evidenze audio/video, fatti salvi gli obblighi di denuncia alle autorità competenti.

Alcune raccomandazioni di buon senso:

- I supporti rimovibili (CD, DVD, pen drive, schede di memoria, hard disk rimovibili, etc.) devono essere custoditi con la massima diligenza e riservatezza e non devono essere lasciati incustoditi o facilmente accessibili.

#### **4.12 Comportamenti non consentiti**

Sono vietati a tutti gli Utenti i seguenti comportamenti:

- a) l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo della smart card di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche della ASL e/o lo scambio di comunicazioni mediante falsa identità;
- b) l'installazione, sulla PdL in dotazione, di software non coperto da licenza o, comunque, non preventivamente autorizzato;
- c) l'utilizzo, per comunicazioni relative alla piattaforma bodycam, di chat, social network o altri strumenti di comunicazione aziendale messi a disposizione dalla ASL;
- d) l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata di file e di ogni altra risorsa informatica;
- e) l'allontanamento dalle PdL senza la preventiva adozione di opportune precauzioni di sicurezza (ad es. il blocco della PdL);
- f) il mantenimento delle PdL accese al termine della attività lavorativa;

- g) la modifica delle configurazioni di base dei dispositivi assegnati dalla ASL senza l'autorizzazione;
- h) l'utilizzo di strumenti volti a eludere i sistemi di protezione.

#### **4.13 Protezione contro furti e danneggiamenti**

Tutte le PdL portatili e i dispositivi mobili, le bodycam e le docking station devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in esse contenuti.

L'Utente è tenuto a informare immediatamente il dirigente responsabile, l'U.O.C. Servizio Informativo Aziendale e, qualora vi sia la possibilità di una violazione di dati personali, altresì il RPD di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

## **5. CONTROLLI E MONITORAGGI**

La piattaforma bodycam imposta la propria azione di monitoraggio e controllo sulle connessioni entranti ed uscenti dalla piattaforma web, dalle docking station e dalle bodycam messe a disposizione per lo svolgimento dell'attività lavorativa. Queste attività sono svolte nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte degli Utenti, adottando in ogni caso le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti.

A tal fine, utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti "file di log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati e delle informazioni ivi contenute.

Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log file relativi possono essere esaminati dagli amministratori di sistema per l'individuazione del problema tecnico e l'adozione delle necessarie misure conseguenziali.

L'amministratore di sistema, nel caso in cui rilevi anomalie, può provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi in concessione alla ASL.

Le predette attività sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

### **5.1. Ruolo degli amministratori delle risorse tecnologiche condivise e delle applicazioni**

Gli Amministratori delle risorse tecnologiche condivise e delle applicazioni svolgono le attività necessarie per garantire la salvaguardia del sistema informativo e delle applicazioni conformemente alle politiche e alle istruzioni impartite dalla ASL e nel



rispetto della normativa vigente con particolare riferimento alla protezione dei dati personali.

Qualora si renda necessario procedere a operazioni finalizzate al ripristino della funzionalità del Sistema informativo comportanti l'accesso a cartelle, file o archivi di altri Utenti, gli Amministratori sono tenuti a preavvisare gli interessati, limitando il proprio intervento a quanto strettamente necessario.

## 6. RESPONSABILITÀ E SANZIONI

La violazione del presente disciplinare e dei Codici di comportamento del personale può comportare l'applicazione delle sanzioni disciplinari previste dal decreto legislativo 30 marzo 2001, n. 165 e s.m.i., dai contratti collettivi applicabili al personale in servizio e dal singolo contratto di lavoro.

Resta ferma la responsabilità civile, penale e contabile di ogni Utente per fatti illeciti e/o danni derivanti da usi non consentiti della Rete o degli strumenti informatici messi a disposizione dalla ASL, anche alla luce delle prescrizioni contenute nel presente disciplinare.

## 7. PRIVACY E DATA PROTECTION

Nella definizione delle regole e delle condizioni per l'utilizzo degli strumenti bodycam della ASL da parte dei soggetti elencati nel presente documento, l'Azienda ha tenuto conto dei profili impattanti in materia di *privacy* e *data protection*, adottando molteplici garanzie e misure di sicurezza tecniche e organizzative volte al rispetto del Regolamento UE 2016/679 (GDPR) e del D.Lgs. 196/2003 (Codice Privacy) ss.mm.ii., nonché di quanto disposto e indicato dall'Autorità Garante per la Protezione dei Dati Personali.

In particolare, nell'ambito del trattamento in oggetto sono trattate le seguenti categorie di dati personali: **(i)** immagini e audiovideo; **(ii)** dati anagrafici degli operatori sanitari che indossano le Bodycam; **(iii)** dati di identificazione elettronica; **(iv)** dati relativi sulla salute e sanitari indiretti. I dati personali sono riferibili alle seguenti categorie d'interessati: **(i)** pazienti; **(ii)** utenti; **(iii)** persone particolarmente vulnerabili; **(iv)** minori; **(v)** dirigenti; **(vi)** dipendenti - operatori sanitari.

Tutti i soggetti interessati coinvolti nel trattamento nascente dall'adozione dei dispositivi Bodycam sono appositamente informati sulla base di una stratificazione delle informazioni privacy, ex art. 13 GDPR, che comprendono rispettivamente: **(i)**

informazioni privacy somministrate al personale utilizzatore della Bodycam; **(ii)** informazioni privacy rivolte all'utenza mediante il sito web istituzionale dell'Azienda; **(iii)** cartellonistica, in forma di “*Graphic-Info*”, con informazioni minime che sono affisse nei locali di interesse della ASL Salerno e che, inoltre, potranno essere affisse sui mezzi adibiti all'emergenza urgenza e/o sulle uniformi degli operatori sanitari sottoforma di *badge*. Queste ultime informazioni contengono un rimando al documento informativo più esteso e dettagliato presente sul sito web istituzionale.

Per quanto attiene alle misure di sicurezza tecniche ed organizzative, in ossequio a quanto disposto dall'art. 32 GDPR, l'Azienda ha implementato le seguenti garanzie che dovranno essere rispettate dal personale utilizzatore:

- l'attivazione della Bodycam avviene solamente mediante pressione del “tasto funzione” posizionato sulla sagoma della stessa da parte dell'operatore, e mai da remoto, previo avviso del medesimo operatore verso il potenziale aggressore e nei soli casi di concreto pericolo;
- l'avvenuta attivazione della registrazione video della Bodycam è comprovata dall'emissione di un segnale sonoro e luminoso;
- i contenuti generati vengono cifrati con chiave asimmetrica (AES-256) e memorizzati su memoria locale del dispositivo. Successivamente il dispositivo viene collegato materialmente alla postazione (dockstation) per permettere il passaggio dei file, su canale sicuro, nell'archivio centrale nel Cloud Microsoft Azure, sito in territorio europeo e, nello specifico in Italia, a Milano;
- l'operatore che registra le immagini attraverso il dispositivo indossabile, come anche l'operatore di postazione che procede alle operazioni del punto precedente, non ha la possibilità di visionare le immagini, né tantomeno di modificarle in alcun modo;
- la bodycam in esercizio non conserva né mostra dati personali di associazione con l'utente, l'assegnazione viene assicurata tramite il solo ID univoco interno al sistema;
- lo schermo posteriore della Bodycam è impostato in modalità “off” per configurazione di sistema predefinita, quindi, non consente la visualizzazione di quanto registrato all'operatore medesimo;
- l'acquisizione multimediale è cifrata e marcata con sovraimpressione e ogni

contenuto multimediale è firmato con generazione di hashing;

- i filmati e i contenuti multimediali ripresi con le Bodycam e raccolti nel sistema sono protetti da cifratura e possono essere consultati dai soli operatori autorizzati a tale attività trattamentale, utilizzando esclusivamente lo specifico software viewer;
- in caso di necessità di consegna del contenuto multimediale all'Autorità giudiziaria, il sistema permetterà di generare un file non cifrato che sarà salvato sulla postazione dell'utente autorizzato all'estrazione, consentendo, al contempo, la registrazione nei file di log delle azioni di richiesta, di generazione e download del file;
- il fornitore della tecnologia è correttamente individuato quale responsabile del trattamento, ai sensi dell'art. 28 GDPR, con annessa individuazione dei sub-responsabili del trattamento che intervengono nelle attività trattamentali rispetto all'affidamento. Mentre i singoli operatori sono designati dal titolare quali persone autorizzate al trattamento ex art. 29 GDPR;
- la conservazione delle immagini avviene esclusivamente per il termine necessario al raggiungimento delle finalità di trattamento, e comunque non oltre le 48 ore successive al deposito della bodycam in docking station – salvo casi di comprovata necessità di conservazione per un termine più ampio –, nel rispetto dei principi di minimizzazione, limitazione della conservazione e limitazione della finalità di trattamento, art. 5 GDPR.

In conclusione, si rappresenta che, in ossequio alle disposizioni normative di settore, l'Azienda Sanitaria di Salerno ha proceduto ad effettuare tutte le attività doverose e diligenti nell'ottica della piena *compliance* normativa mediante la produzione di apposita documentazione e, nello specifico: **(i)** informazioni privacy come sopra dettagliatamente elencate; **(ii)** nomina a Responsabile del Trattamento ex art. 28 GDPR del fornitore dei dispositivi e della piattaforma; **(iii)** valutazione d'impatto sui diritti e le libertà delle persone fisiche (DPIA) ex art. 35 GDPR.