



# DPIA

*ex art. 35 GDPR*

## Sommario

### **IL CONTESTO NORMATIVO DEL DATA PROTECTION IMPACT**

#### **ASSESSMENT ..... 3**

#### **Data Protection Impact Assessment..... 10**

#### **(DPIA) ..... 10**

#### **A. CONTESTO..... 10**

#### **VALUTAZIONE DEL RISCHIO INERENTE ..... 19**

##### **ACCESSO ILLEGITTIMO ..... 21**

##### **MODIFICA INDESIDERATA..... 23**

##### **PERDITA ACCIDENTALE ..... 25**

#### **CALCOLO DEL RISCHIO INERENTE ..... 26**

#### **B. MISURE DI SICUREZZA ..... 28**

##### **B.2) MISURE DI SICUREZZA TECNICHE..... 29**

#### **VALUTAZIONE DEL RISCHIO RESIDUO ..... 33**

##### **ACCESSO ILLEGITTIMO ..... 33**

##### **MODIFICA INDESIDERATA..... 36**

##### **PERDITA ACCIDENTALE ..... 37**

#### **VALUTAZIONE DEL RISCHIO RESIDUO ..... 39**

##### **CALCOLO DEL RISCHIO RESIDUO DEL TRATTAMENTO..... 39**

#### **PARERE DEL DPO ..... 40**

# IL CONTESTO NORMATIVO DEL DATA PROTECTION IMPACT ASSESSMENT

Il *Data Protection Impact Assessment* (per brevità anche DPIA) è uno strumento importante in termini di responsabilizzazione (*principio di accountability*), in quanto soccorre e sostiene il Titolare del trattamento non soltanto nel rispettare e far rispettare le prescrizioni del GDPR, ma anche nel dimostrare di aver adottato le misure idonee a mitigare il rischio durante tutte le fasi trattamentali. In altri termini, la Valutazione d'Impatto sulla Protezione dei Dati è una procedura di *risk management* che permette di dimostrare la conformità con le norme in materia di protezione dei dati personali europee e domestiche. Muovendo i passi dal dettato normativo, segue il testo dell'art. 35 GDPR:

“ART. 35

## Valutazione d'impatto sulla protezione dei dati

*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.”*

La disciplina sulla DPIA, contenuta nel GDPR, deve essere integrata anche da quanto specificato dal WP29 (oggi *European Data Protection Board* - EDPB) nelle linee guida concernenti la valutazione di impatto sulla protezione dei dati, nonché i criteri per stabilire se un trattamento possa o meno presentare un rischio privacy più o meno elevato.

In particolare, le linee guida citate ampliano l'obbligatorietà della valutazione di impatto, oltre ai casi espressamente indicati dal regolamento all'art. 35, par. 3, GDPR, anche in quelli che comportano la comunicazione di dati su larga scala tra diversi titolari e/o trattamenti sistematici di dati genetici o sanitari, tenendo conto del volume dei dati, della durata e dell'attività di trattamento.

Il presente documento è, inoltre, uno strumento dedicato alla valutazione del rischio ed ha lo scopo di fornire informazioni basate sia su evidenze che su metodi di analisi, al fine di rendere agevole l'adozione di decisioni informate circa il trattamento di particolari rischi. Le informazioni ottenute consentono, quindi, di identificare i fattori determinanti, gli eventi potenzialmente dannosi e suggerire le azioni correttive possibili da mettere in atto per prevenire la ripetizione degli eventi stessi.

Nella prospettiva della gestione del rischio privacy, tale documento risponde al principio fondamentale dell'*accountability*, intesa quale dimostrazione di come il titolare del trattamento abbia posto in essere tutte le misure di sicurezza volte a tutelare i diritti e le libertà degli interessati.

La responsabilizzazione, quale obbligo di rendere conto di ciò che si fa e ciò che si fa fare, rappresenta il fulcro della nuova frontiera della privacy in quanto aspetto essenziale per l'esercizio di una corretta ed efficace *governance*.

Il Regolamento UE 2016/679 pone, altresì, la necessità di rendere conto anche dell'adozione di comportamenti proattivi, tali da *"dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR"* (artt. 23-25, in particolare, e l'intero Capo IV del GDPR).

Ne consegue, dunque, che è affidato al Titolare del trattamento dei dati il compito di decidere autonomamente le modalità, le misure di sicurezza e i limiti del trattamento stesso, nel rispetto delle disposizioni normative ed alla luce dei criteri indicati nel Regolamento UE, oltre che a quelli indicati dall'ordinamento interno (Codice Privacy - D.lgs. 196/2003, come

novellato dal D.lgs. 101/2018) e rispetto alle Linee Guida e Regole Deontologiche previste dal Garante per la Protezione dei Dati Personali.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by design and by default*" (art. 25 GDPR), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio e per impostazione predefinita le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento stesso e tutelare i diritti e le libertà degli interessati, tenendo conto del contesto complessivo ove il trattamento viene svolto e dei rischi connessi.

Fondamentali fra tali attività sono quelle relative al successivo criterio del rischio inerente al trattamento; quest'ultimo è da ritenersi, infatti, come il rischio capace di impattare negativamente sulle libertà e sui diritti degli interessati (considerando 75-77).

Tali criticità dovranno essere analizzate attraverso un apposito processo di valutazione (artt. 35 e 36 GDPR) tenendo conto dei rischi noti o ipotizzabili e delle misure tecniche, fisiche e organizzative che il Titolare ritiene di dover adottare per mitigare tali rischi.

In ossequio a tali criteri, il presente documento viene redatto in base alle tecniche ed alle modalità della norma ISO/IEC 31000:2018, "*Risk Management – Principles and guidelines*", che descrive in dettaglio il processo logico e sistematico che porta alla mitigazione e controllo dei rischi.

La *ratio* della scelta risiede nella necessità di conferire connotati positivi alla gestione del rischio, anche attraverso la percezione dello stesso come opportunità, mediante una lettura del pericolo quale possibilità di innovazione.

Ulteriore ed importante elemento di valutazione è il contenuto dello standard ISO/IEC 31010:2009 (*Risk Management e Risk Assessment Techniques*) ove vengono riportati i concetti della gestione dei rischi e le diverse tecniche atte alla loro valutazione nei diversi ambiti.

È, infine, doveroso adeguarsi alle disposizioni contenute nelle norme:

ISO/IEC 29134:2017 ("*Information technology — Security techniques — Guidelines for privacy impact assessment*") che indica linee guida applicabili a tutte le tipologie di

- ▶ strutture, pubbliche e private, al fine di creare, organizzare ed implementare progetti GDPR *compliant*;
- ▶ ISO/IEC 27002:2017 ("*Information Technology - Security techniques - Code of practice for information security controls*") che indica le linee guida per gli standard di sicurezza delle informazioni organizzative e pratiche di gestione della sicurezza delle informazioni, compresa la selezione, l'implementazione e la gestione dei controlli;
- ▶ ISO/IEC 27005:2018 ("*Information security risk management*") che, è in parte applicabile anche alla valutazione del rischio connesso al trattamento dei dati personali; assumono importanza determinante le appendici dedicate all'approfondimento di alcuni aspetti della gestione dei rischi e, in particolare, quella relativa al catalogo delle minacce;
- ▶ ISO/IEC 27701:2019 ("*Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines*") che fornisce requisiti e linee guida per costruire, implementare, mantenere e migliorare costantemente un PIMS (*Privacy Information Management System* o sistema di gestione delle informazioni sulla privacy), sia qualora l'organizzazione operi come titolare del Trattamento (*Data Controller*), che come Responsabile (*Data Processor*).
- ▶ ISO 31000:2018 ("*Risk management -- Principles and guidelines*") fornisce principi e linee guida generali per la gestione del rischio ed è applicabile a tutte le tipologie di organizzazioni. La ISO 31000 può essere applicata a qualsiasi tipo di rischio e nel corso dell'intero ciclo di vita di un'organizzazione, in merito a molteplici attività come la definizione di strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni.

In conclusione, il rischio può essere definito come la combinazione delle probabilità di un evento e della gravità delle sue conseguenze. Qualunque tipo di iniziativa implica potenzialmente eventi e conseguenze che rappresentano possibili benefici (elementi

positivi) o minacce alla sicurezza dell'attività trattamentale posta in essere (elementi negativi).

I principali impatti sui diritti e le libertà degli interessati, qualora il rischio di accesso illegittimo, modifica indesiderata e/o perdita di dati dovesse concretizzarsi, sono rappresentati da:

- perdita del controllo dei dati personali;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione d'identità;
- frodi;
- perdite finanziarie;
- decifratura non autorizzata alla pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- conoscenza da parte di terzi non autorizzati;
- qualsiasi altro danno economico o sociale significativo;
- danni fisici o psicologici.

Le principali minacce che potrebbero concretizzare il rischio di accesso illegittimo, modifica indesiderata e/o perdita dei dati personali consistono in:

- danni fisici, ossia azioni offensive finalizzate a distruggere, esporre, alterare, disabilitare, sottrarre o ottenere l'accesso non autorizzato a risorse fisiche come l'infrastruttura, l'hardware o l'interconnessione. Rientrano in questa categoria atti di



vandalismo, furto, sabotaggio, perdita di informazioni e attacchi massivi riguardanti qualsiasi tipo di infrastruttura, anche quella Internet;

- eventi naturali, ossia eventi che possono distruggere, danneggiare o rendere irrecuperabili risorse fisiche come l'infrastruttura, l'hardware o l'interconnessione (ad esempio fenomeni climatici, incendi, allagamenti, ecc.);
- perdita di servizi essenziali, ossia interruzioni, perdite o malfunzionamenti dei servizi accessori fondamentali per il corretto funzionamento dell'infrastruttura hardware o di interconnessione alle reti informatiche e dati (ad esempio interruzioni nei collegamenti di rete, blackout);
- disturbi, ossia disturbi elettromagnetici o di contorno che possono causare interruzioni o malfunzionamenti dell'infrastruttura hardware o di interconnessione (ad esempio disturbi di rete di tipo intermittente o continuo);
- compromissione di informazioni, ossia azioni mirate ad ascoltare, interrompere o prendere il controllo di una comunicazione di terzi senza il consenso. Le minacce 'legali' comprendono la violazione di norme e leggi, nonché il mancato rispetto dei requisiti contrattuali da parte di prestatori di servizi verso gli utilizzatori dell'infrastruttura di rete (ad esempio furto di documenti o di supporti di memorizzazione);
- problemi tecnici, definiti come guasto o malfunzionamento. Ne sono esempi guasti o interruzioni di dispositivi di rete o sistemi, bug di software o errori di configurazione. Le 'interruzioni' sono disordini inattesi del servizio o riduzione della qualità che scendono al di sotto di un livello richiesto (ad esempio problemi ai software, uso dei servizi da parte di persone non autorizzate);
- azioni non autorizzate, ossia azioni che mirano ai sistemi, alle infrastrutture e/o alle reti mediante azioni dannose. Le minacce comuni sono generalmente definite come attacchi informatici e azioni correlate (ad es. spam, malware, spyware, botnet,



manipolazione di hardware e software, alterazioni delle configurazioni, DDoS, sfruttamento di bug dei software, violazione di dati, furto di identità);

- compromissione di funzioni, ossia un danno involontario o accidentale che si riferisce a distruzione, danni fisici e perdite di informazioni per lo più dovuti ad alterazioni del sistema o all'utilizzo inadeguato dei sistemi;
- attacchi di ingegneria sociale, ossia danni veicolati attraverso una serie di tecniche basate su processi cognitivi di influenzamento, inganno e manipolazione che, sfruttando l'ingenua disponibilità e buona fede, nonché l'ignoranza e poca attenzione della vittima, sono finalizzate all'ottenimento di informazioni riservate o sensibili (ad esempio attacchi phishing, divulgazione involontaria delle informazioni).

# Data Protection Impact Assessment (DPIA)

Titolare del trattamento: *ASL Salerno*

Nome Attività: *Sistema per la prevenzione e contrasto degli atti di violenza a danno degli esercenti le professioni sanitarie ("bodycam")*

Data di creazione: *11 marzo 2024*

Data Rev 01: *27 maggio 2024*

Data Rev 02: *23 luglio 2024*

Data Rev 03: *6 agosto 2024*

Data Rev 04: *20 agosto 2024*

## A. CONTESTO

Il tema della sicurezza e della prevenzione degli atti di violenza nelle Aziende Sanitarie è un tema costante e costituisce un preciso dovere del datore di lavoro che ha l'obbligo di assicurare un ambiente lavorativo sicuro e salubre in favore tanto dei dipendenti, quanto in favore dei pazienti e dei loro familiari.

Gli episodi di violenza e vandalismo in aree critiche e strategiche delle Aziende Sanitarie rappresentano un fenomeno che si ripete nel tempo e che viene generalmente arginato in ottica preventiva attraverso strumenti *ad hoc*, si veda per esempio la videosorveglianza e i sistemi di allarme. Tali strumenti, in ossequio alle previsioni di legge (tanto in materia giuslavoristica, quanto in materia privacy e data protection) passano necessariamente attraverso step predefiniti e garantisti al fine di ponderare e bilanciare tutti gli interessi e i diritti in gioco.

Non sempre, tuttavia, gli strumenti a disposizione delle pubbliche amministrazioni risultano idonei, però, a garantire la sicurezza necessaria ad arginare i vari scenari possibili, tenuto conto del contesto, anche ambientale, oppure tenuto conto del rischio e della probabilità che un determinato fenomeno violento accada.

Dunque, il tema della violenza sugli operatori sanitari è ormai da considerarsi una criticità quotidiana, la quale ha avuto un deciso aumento con l'exasperazione generale causata dallo stato di isolamento dovuto dalla pandemia che ha inevitabilmente determinato un aumento delle patologie legate ai disturbi dell'umore e ad una maggiore aggressività verso gli operatori sanitari.

Per tali ordini di motivi, si ritiene fondamentale agire in maniera più incisiva attraverso misure di sicurezza più efficaci, sempre garantendo il rispetto dei diritti fondamentali delle persone, laddove i classici strumenti dissuasivi non risultino più idonei.

Il dispositivo c.d. bodycam indossato dall'operatore sanitario della ASL Salerno che opera rispettivamente nelle:

- 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);

e che, dunque, è esposto a situazioni di rischio, è specificamente progettato allo scopo di documentare situazioni che possano mettere in pericolo l'incolumità degli operatori stessi e/o dei pazienti e, implicitamente, prevenire tali evenienze e contrastare le aggressioni, i furti e gli atti vandalici. Il Dispositivo è ideato secondo una logica *privacy by design* ed è rispettoso delle indicazioni del Garante per la Protezione dei Dati Personali rilasciate attraverso pareri e provvedimenti sul tema.

La procedura operativa prevede l'attivazione della bodycam mediante pressione di più tasti funzione agilmente posizionati sulla sagoma della stessa; il dispositivo conferma l'avvenuta attivazione mediante l'emissione di un segnale, sia sonoro che luminoso. I contenuti generati vengono memorizzati sulla memoria locale del dispositivo per essere poi trasferiti, tramite apposita postazione (docking station) nell'archivio centrale in cloud sito in territorio europeo, nello specifico in Italia, a Milano (Cloud Microsoft Azure).

Di seguito si elencano, a titolo riepilogativo, le principali misure tecniche ed organizzative sottostanti la soluzione:

- l'attivazione della bodycam avviene solamente mediante pressione dei “tasti funzione” posizionati 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 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, 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;
- il sistema non permette l'avvio della registrazione, compromettendone la funzionalità di ripresa, se alla bodycam non è stato preventivamente associato alcun codice ID operatore;

- 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 la riproduzione è marcata con sovraimpressione dell’ID operatore, inoltre, 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 *de quo*. Mentre i singoli operatori sono designati dal titolare del trattamento quali persone autorizzate al trattamento ex artt. 29 GDPR e 2-quaterdecies Codice Privacy.

La conservazione delle immagini avviene esclusivamente per il termine necessario al raggiungimento delle finalità di trattamento, e comunque non oltre 48 ore nel rispetto dei principi di minimizzazione, limitazione della conservazione e limitazione della finalità di trattamento (art. 5 GDPR).

#### **CASI CONCRETI DI ATTIVAZIONE DELLA VIDEORIPRESA:**

- UOC EMERGENZA - COT 118 - URGENZA TERRITORIALE:
  - Aggressioni fisiche e/o verbali da parte della persona soccorsa e/o di familiari e/o di terzi presenti sul luogo all’arrivo del servizio di emergenze-urgenza;

- Aggressioni fisiche e/o verbali da parte della persona soccorsa durante il trasporto ovvero aggressioni e/o atti violenti nei confronti del guidatore;
- UOSD TUTELA SALUTE ADULTI E MINORI AREA PENALE:
  - Aggressioni fisiche, minacce e/o similari da parte del soggetto detenuto durante la visita medica;
- UOSD SERVIZIO PSICHIATRICO DI DIAGNOSI E CURA (SPDC):
  - Gestione di pazienti con disturbi psichiatrici che mostrano comportamenti violenti su persone o cose;
  - Comportamenti autolesionistici dei pazienti con disturbi psichiatrici;
  - Comportamenti suicidari dei pazienti con disturbi psichiatrici;
  - Aggressioni fisiche e/o verbali a causa della mancata volontà di assumere i farmaci;
  - Aggressioni fisiche e/o verbali a causa del cambio del terapeuta;
- PRONTO SOCCORSO IN AREA DI COMPETENZA SPDC:
  - aggressioni verbali o fisiche da parte di pazienti, familiari o visitatori;
  - gestione di pazienti aggressivi a causa di uso di sostanze stupefacenti;
  - risse e aggressioni fisiche tra pazienti, tra pazienti e operatori sanitari, tra visitatori e operatori sanitari all'interno del P.S.

La videoripresa viene realizzata esclusivamente nelle gravi situazioni di rischio sopra esplicate.

#### **CASI IN CUI L'AUDIO RISULTEREBBE NECESSARIO RISPETTO ALLE FINALITA':**

- Aggressioni verbali, minacce e/o similari da parte di pazienti e/o visitatori nei confronti del personale sanitario ovvero nei confronti di altri pazienti o visitatori.

La raccolta delle immagini audio-video non è costante, infatti, la registrazione del video e del relativo audio, avviene esclusivamente al presentarsi della situazione di pericolo e/o violenta ed esclusivamente a seguito di attivazione della bodycam da parte dell'operatore.

Gli operatori sono opportunamente formati e istruiti al fine di riconoscere le situazioni e i

casi in cui dovranno essere attivate le bodycam e sarà vietato ogni uso difforme dalle istruzioni sopra richiamate.

### **1) Finalità del trattamento:**

- ✓ Sicurezza nell'ottica della prevenzione e contrasto degli atti di violenza a danno degli esercenti le professioni sanitarie attraverso l'utilizzo dei sistemi di "bodycam"

### **2) Categorie di interessati:**

- ✓ Pazienti
- ✓ Utenti
- ✓ Persone particolarmente vulnerabili
- ✓ Minori
- ✓ Dirigenti
- ✓ Dipendenti/Operatori Sanitari

### **3) Numero di interessati:**

- ✓ Oltre i 1000

### **4) Sono somministrate le informazioni privacy all'interessato?**

- ✓ Sì

### **5) Come sono rese all'interessato le informazioni privacy?**

- ✓ Informazioni privacy somministrate al personale utilizzatore della bodycam all'avvio dell'utilizzo del sistema
- ✓ Informazioni privacy estese e dettagliate pubblicizzate mediante il sito istituzionale della ASL Salerno
- ✓ Cartellonistica - Graphic-Info, con informazioni minime affisse nei locali di interesse della ASL Salerno, con l'inserimento di uno strumento digitale (link oppure Qr Code) di rimando al documento informativo più esteso e dettagliato presente sul sito web istituzionale.



**6) Sono previste modalità per l'esercizio dei diritti dell'interessato? (quali, il diritto di accesso, di rettifica, di cancellazione, di limitazione, di portabilità dei dati, di opposizione)**

- ✓ Si, risulta non applicabile il diritto alla portabilità

**7) Quali sono le modalità per l'esercizio dei diritti dell'interessato?**

- ✓ Tramite raccomandata A/R
- ✓ A mezzo mail/PEC

**8) Categorie di dati personali:**

- ✓ Immagini e audiovideo
- ✓ Dati anagrafici degli operatori sanitari che indossano le bodycam
- ✓ Dati di identificazione elettronica
- ✓ Dati relativi sulla salute e sanitari, anche indiretti

**9) Elencare le attività di trattamento effettuate:**

- ✓ Raccolta
- ✓ Registrazione
- ✓ Conservazione
- ✓ Elaborazione
- ✓ Estrazione
- ✓ Consultazione
- ✓ Utilizzo
- ✓ Comunicazione
- ✓ Cancellazione
- ✓ Distruzione

**10) Modalità di conservazione:**

- ✓ Digitale

**11) Cancellazione:**

- ✓ Fino al raggiungimento delle finalità di trattamento

- di *default* i *file* audio-video sono conservati per un termine limitato, non oltre le 48 ore, con cancellazione automatica e irreversibile degli stessi una volta decorso il tempo di conservazione previsto
- nelle ipotesi in cui si configuri la necessità di conservare i *file* audio-video per un tempo superiore, anche per ragioni di giustizia su indicazione dell'Autorità Giudiziaria, è prevista la possibilità di estrapolare i *file* oppure di selezionare i *file* d'interesse e bloccare la cancellazione automatica predefinita, rendendo i *file* cancellabili esclusivamente allo scadere di un nuovo *alert* e in maniera manuale. Tale processo avviene previa verifica e valutazione da parte del personale autorizzato e della Governance circa la rilevanza delle immagini raccolte per le suddette finalità

## **12) Categorie di destinatari:**

- ✓ Responsabile del trattamento *ex art. 28* GDPR (Almaviva S.p.a. con sub-responsabile del trattamento Intellicare S.r.l.)
- ✓ Autorità di Giustizia (eventuale)
- ✓ Forze dell'Ordine Pubblico (eventuale)

## **13) Piattaforme, dispositivi e/o applicativi utilizzati nell'ambito dell'attività di trattamento in esame:**

- bodycam, pc, *Database server*; piattaforma *web based*; *cloud*; *datacenter*; *software* IBWC (integra taluni servizi, funzionali alla comunicazione con le *docking station* di ricarica, con le bodycam e con i *client web*)

## **14) Avviene un trasferimento di dati personali al di fuori dei confini nazionali?**

- ✓ Non applicabile

## **15) Base giuridica del Trattamento *ex art. 6* GDPR:**

- ✓ Adempimento di un obbligo legale (art. 6, par. 1, lett. c) (art. 88 GDPR, nonché art. 114 Codice Privacy, in riferimento all'art 4 della Legge n. 300 del 1970)

## **16) Base giuridica del trattamento ex art. 9 GDPR:**

- ✓ Assolvimento degli obblighi ed esercizio dei diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (art. 9, par. 2, lett. b), fondato sulla normativa nazionale di riferimento (Legge n. 300 del 1970 – D. Lgs. n. 81 del 2008)

## **17) Tipologia di trattamento:**

- ✓ Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti

## **18) Vengono applicate e/o osservate linee guida, best practice di settore, norme UNI/ISO/IEC, codice di condotta, regolamenti aziendali, etc.?**

- ✓ Sì, Intellitronika S.r.l., produttore delle bodycam, è certificata ISO 9001:2015, ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO 14001:2015; il dispositivo bodycam è certificato Directive 2014/53/EU EU Type Examination Certificate Notified Body: 1313 da BACL (Bay Area Compliance Labs Corp.); i *datacenter* del fornitore Azure sono certificati ISO 27001, ISO 27018, SOC 1, SOC 2, SOC 3, FedRAMP, HITRUST, MCTS, IRAP, ENS; policy sul corretto utilizzo delle bodycam

## **19) Quali sono? Elencare:**

- Linee guida EDPB n. 3/2019
- Provvedimento Garante 8 aprile 2010
- Raccomandazione Ministero della Salute 19 novembre 2007, n. 8
- L. 14 agosto 2020, n. 113

## **20) La finalità di trattamento è specifica, esplicita e legittima?**

- ✓ **Specifica:** è ben delineata ed individuata nella necessità da parte del titolare del trattamento di espletare l'attività di videosorveglianza a mezzo di bodycam attivabili in situazioni di pericolo, al fine di garantire la tutela degli asset aziendali, dei

dependenti, degli utenti e dei pazienti, nonché ridurre e prevenire eventi violenti nei confronti di cose e/o persone

- ✓ **Eslicita:** in quanto rappresentata chiaramente agli interessati per il tramite delle informazioni privacy ex art. 13 GDPR, sotto forma anche di cartellonistica apposta nei locali interessati della ASL
- ✓ **Legittima:** in quanto sorretta da un'idonea base giuridica, rappresentata dall'art. 6, par. 1, lett. c), nonché dall'art. 9, par. 2, lett. b) GDPR fondati sulla normativa nazionale di riferimento (Legge n. 300 del 1970 – D. Lgs. n. 81 del 2008)

## 21) Come viene rispettato il principio di minimizzazione dei dati?

- Sono trattati esclusivamente i dati necessari al perseguimento della finalità del Titolare, consistente nella volontà di garantire la videosorveglianza mediante bodycam attivabili esclusivamente in caso di pericolo. Difatti, i dati personali oggetto di raccolta risultano fondamentali per l'esecuzione dell'attività trattamentale descritta nel contesto; pertanto, i dati raccolti risultano adeguati, pertinenti e limitati rispetto alla specifica finalità.

Difatti, apposite procedure operative limitano l'impiego della bodycam a specifici casi e ad una valutazione condotta dall'operatore esposto al pericolo; la bodycam indossata è di *default* non accesa e attivabile solo dall'operatore in caso di necessità con apposite procedure e non è attivabile da remoto; inoltre, lo schermo della bodycam è disattivato e non permette la registrazione con strumenti ulteriori ed esterni.

## VALUTAZIONE DEL RISCHIO INERENTE

Il livello di **rischio (R)** è determinato dal prodotto della probabilità di accadimento di un evento/minaccia (**P**) per il potenziale impatto sui diritti e le libertà degli interessati (**I**) determinato da tale potenziale evento, laddove dovesse verificarsi.

Per **probabilità** si intende l'eventualità che un rischio identificato o una minaccia possano concretizzarsi.

Per **impatto** si intende in una valutazione delle conseguenze di ciascuna minaccia in termini di potenziali danni o lesioni ai diritti e alle libertà degli interessati.

$$\underline{R = I \times P}$$

Il **rischio inerente** consiste nel calcolo del rischio iniziale, ossia al **netto delle misure di sicurezza** volte a mitigarne i rischi.

L'**impatto** è classificato secondo una scala da 1 a 4; la scala utilizzata per tale valutazione deriva dalla norma ISO 29134 *"Information technology - Security techniques - Guidelines for privacy impact assessment"*.

L'impatto dovrà essere calcolato in rapporto all'eventualità di accesso illegittimo ai dati personali, di modifica indesiderata e perdita dei dati personali, a tutela del principio RID (Riservatezza, Integrità, Disponibilità).

4	Massimo	L'impatto è estremamente grave, con conseguenze irreversibili per gli interessati che potrebbero non superare
3	Significativo	Le conseguenze per gli interessati sono gravi e possono essere mitigate con l'adozione di ulteriori misure di sicurezza
2	Limitato	Le conseguenze per gli interessati, sebbene non trascurabili, sono limitate e possono essere mitigate con misure adeguate
1	Trascurabile	Gli interessati non subiscono conseguenze significative

La **probabilità** è valutata, anch'essa, su di una scala da 1 a 4 e consiste nella frequenza di accadimento di una minaccia.

Anche la probabilità dovrà essere stimata in relazione all'eventuale accesso ai dati personali, alla modifica indesiderata e alla perdita dei dati personali.

4	Massimo	L'evento ha un'alta probabilità di verificarsi
3	Significativo	L'evento ha una probabilità moderata di verificarsi
2	Limitato	L'evento ha una bassa probabilità di verificarsi, la quale non può considerarsi del tutto esclusa
1	Trascurabile	L'evento ha una probabilità estremamente bassa di verificarsi, al punto da poter essere considerato improbabile

## **ACCESSO ILLEGITTIMO**

### **22) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di accesso illegittimo dovesse concretizzarsi?**

- ✓ Perdita del controllo dei dati personali
- ✓ Decifratura non autorizzata alla pseudonimizzazione
- ✓ Pregiudizio alla reputazione
- ✓ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ✓ Conoscenza da parte di terzi non autorizzati

### **23) Quali sono le principali minacce che potrebbero concretizzare il rischio?**

- ✓ Compromissione di informazioni
- ✓ Azioni non autorizzate
- ✓ Attacchi di ingegneria sociale

### **24) Quali sono le principali fonti di rischio?**

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

### **25) Quali sono le principali vulnerabilità che possono determinare l'accesso illegittimo?**

- Assenza di formazione del personale;
- Assenza di crittografia del *database*, dei dispositivi e dei dati in transito;
- Assenza di previsione di un sistema di controllo degli accessi logici;
- Assenza di un'autenticazione forte;
- Assenza di un sistema di sicurezza perimetrale e misure *antivirus/anti-malware*

### Esempi concreti delle principali fonti di rischio che possono determinare un accesso indesiderato ai dati personali:

Scattare foto dello schermo
Copia non autorizzata del contenuto
Visione delle immagini senza essere autorizzati
Recupero di un dispositivo hardware scartato
Sistema di autenticazione non adeguato
Accesso non riservato ai locali delle postazioni fisiche di controllo

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
<div style="display: flex; flex-direction: column; gap: 5px;"> <div><span style="display: inline-block; width: 10px; height: 10px; background-color: green; border: 1px solid black;"></span> 1, 2, 3 TRASCURABILE</div> <div><span style="display: inline-block; width: 10px; height: 10px; background-color: yellow; border: 1px solid black;"></span> 4, 6, 8 LIMITATO</div> <div><span style="display: inline-block; width: 10px; height: 10px; background-color: red; border: 1px solid black;"></span> 9, 12, 16 MASSIMO</div> </div>	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

**$R_i = I(3) \times P(2) \rightarrow 6$  RISCHIO LIMITATO**



## **MODIFICA INDESIDERATA**

**26) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di modifica indesiderata dei dati dovesse concretizzarsi?**

- ✓ Pregiudizio alla reputazione
- ✓ Qualsiasi altro danno economico o sociale significativo
- ✓ Attacchi di ingegneria sociale

**27) Quali sono le principali minacce che potrebbero concretizzare il rischio?**

- ✓ Compromissione di informazioni
- ✓ Azioni non autorizzate

**28) Quali sono le principali fonti di rischio?**

- ✓ Fonti umane interne
- ✓ Fonti umane esterne

**29) Quali sono le principali vulnerabilità che possono determinare la modifica indesiderata?**

- Assenza di formazione del personale;
- Assenza di un sistema di *backup*;
- Assenza di attività di *logging* per verificare modifiche indesiderate

## Esempi concreti delle principali fonti di rischio che inducono una modifica indesiderata dei dati personali:

Errori durante gli aggiornamenti, la configurazione o manutenzione
Infezione da codice malevolo
Rimozione dei componenti essenziali al corretto funzionamento
Errore dell'operatore che modifica i dati
Scarse competenze

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
<div> <div>■</div> 1, 2, 3 TRASCURABILE         </div> <div> <div>■</div> 4, 6, 8 LIMITATO         </div> <div> <div>■</div> 9, 12, 16 MASSIMO         </div>	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

**$R_i = I (2) \times P (2) \rightarrow 4$  RISCHIO LIMITATO**

## **PERDITA ACCIDENTALE**

### **30) Quali potrebbero essere i principali impatti sui diritti e le libertà degli interessati se il rischio di perdita di dati dovesse concretizzarsi?**

- ✓ Limitazione dei diritti
- ✓ Qualsiasi altro danno economico o sociale significativo;
- ✓ Possibile conoscenza da parte di terzi non autorizzati;

### **31) Quali sono le principali minacce che potrebbero concretizzare il rischio?**

- ✓ Danni fisici
- ✓ Eventi naturali
- ✓ Perdita di servizi essenziali
- ✓ Disturbi
- ✓ Azioni non autorizzate
- ✓ Compromissione di funzioni

### **32) Quali sono le principali fonti di rischio?**

- ✓ Fonti umane interne
- ✓ Fonti umane esterne
- ✓ Fonti non umane

### **33) Quali sono le principali vulnerabilità che possono determinare la perdita dei dati personali?**

- Assenza di formazione del personale;
- Assenza di un sistema di *backup*;
- Assenza di aggiornamenti dei sistemi operativi;
- Assenza di crittografia del *database*, del dispositivo e dei dati in transito;
- Assenza di un sistema di sicurezza perimetrale, antivirus/anti-malware;
- Assenza di un sistema di monitoraggio e *logging*

## Esempi concreti delle principali fonti di rischio che inducono una perdita dei dati personali:

Interruzione di corrente
Surriscaldamento eccessivo
Attacco informatico
Inondazioni, incendi, atti vandalici, danni naturali, usura, malfunzionamento del dispositivo
Errori del personale che accidentalmente cancella i dati
Errore durante gli aggiornamenti

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
<div>■ 1, 2, 3 TRASCURABILE</div> <div>■ 4, 6, 8 LIMITATO</div> <div>■ 9, 12, 16 MASSIMO</div>	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

**$R_i = I(3) \times P(2) \rightarrow 6$  RISCHIO LIMITATO**


## CALCOLO DEL RISCHIO INERENTE

AREE DI RISCHIO	STIMA IMPATTO	STIMA PROBABILITA'
RISERVATEZZA	GRAVE	POCO PROBABILE
INTEGRITA'	MEDIO	POCO PROBABILE
DISPONIBILITA'	GRAVE	POCO PROBABILE
VALUTAZIONE (si prende in considerazione il valore più alto tra le valutazioni riferite alle voci RID)	3	2

# VALUTAZIONE RISCHIO INERENTE DEL TRATTAMENTO

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
<div>■ 1, 2, 3 TRASCURABILE</div> <div>■ 4, 6, 8 LIMITATO</div> <div>■ 9, 12, 16 MASSIMO</div>	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

**$R_i = I (3) \times P (2) \rightarrow 6$  RISCHIO LIMITATO**

	TRASCURABILE	Combina bassa probabilità e basso impatto
	LIMITATO	Combina probabilità e impatto moderati
	SIGNIFICATIVO	Combina alta probabilità e impatti significativi
	MASSIMO	Combina probabilità massima e impatti critici

## **B. MISURE DI SICUREZZA**

Una volta calcolato il rischio inerente (iniziale), si procede con l'identificazione delle misure di sicurezza tecnico-organizzative da adottare al fine di mitigare il livello di rischio calcolato in astratto e, di conseguenza, valutarne l'efficacia in concreto.

### **B.1) MISURE DI SICUREZZA ORGANIZZATIVE**

<b><u>Sicurezza dell'archiviazione della documentazione cartacea</u></b>	Non applicabile
<b><u>Nomina delle Persone autorizzate per designazione</u></b>	Si
<b><u>Nomina dei delegati al trattamento</u></b>	Si
<b><u>Nomina dei Responsabili del trattamento</u></b>	Si
<b><u>Elaborazione ed adozione di policy privacy aziendali</u></b>	Si
<b><u>Controllo degli accessi fisici</u></b>	Si
<b><u>Quali strumenti vengono utilizzati per il controllo degli accessi fisici?</u></b>	Presenza di personale all'interno delle postazioni autorizzato alla visualizzazione delle immagini provenienti dalle bodycam
<b><u>Formazione del personale</u></b>	Si
<b><u>Altra misura di sicurezza fisica e/o organizzativa implementata</u></b>	Non Applicabile

## **B.2) MISURE DI SICUREZZA TECNICHE**

<b><u>Crittografia Database</u></b>	Crittografia asimmetrica (i contenuti multimediali presenti nello <i>storage</i> della camera sono cifrati con una chiave pubblica, la cui controparte privata non è presente nella camera stessa; pertanto, anche qualora si dovesse riuscire ad avere accesso ai contenuti della camera, non sarebbe possibile decifrarli per riprodurli)
<b><u>Sistema operativo workstation</u></b>	Windows
<b><u>Aggiornamento sistema operativo</u></b>	Si
<b><u>Configurazione workstation</u></b>	Utente con restrizioni
<b><u>Tecniche di pseudonimizzazione</u></b>	Le immagini sono collegate al numero ID bodycam associata all'operatore che ha ripreso l'evento, nella cui esecuzione sono state registrate; in generale sono altresì collegate all'orario di servizio del personale
<b><u>Partizionamento</u></b>	Non applicabile
<b><u>Controllo degli accessi logici</u></b>	Si



<p><b><u>Quali strumenti per il controllo degli accessi logici vengono utilizzati?</u></b></p>	<p>Possono essere messi in atto protocolli di <i>Strong Authorization</i> con architettura applicativa di riferimento SSO in uso attualmente alla ASL Salerno ; gli operatori che raccolgono le immagini non possono accedervi in alcun modo (schermo oscurato); il cloud su cui sono archiviate le immagini è accessibile solo a specifici soggetti individuati dal direttore di UOC tramite opportuna procedura operativa; l'accesso all'applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali; il sistema sarà connesso con l'AD dell'Amministrazione ed erediterà tutte le policy di autenticazione imposte</p>
<p><b><u>Tracciabilità</u></b></p>	<p>Si (all'interno delle porzioni di <i>Database</i> sono conservati tutti gli accessi alla piattaforma e tutte le richieste di accesso alle informazioni conservate in osservanza al requisito di tracciabilità di ogni operazione di salvataggio, accesso, estrazione dei dati multimediali; l'applicativo implementa un sistema di <i>audit log</i> atto a registrare le attività effettuate dagli utenti e dal sistema (dalla <i>workstation</i> in fase di visualizzazione dei file audio-video il sistema marca in</p>

	sovraimpressione durante la riproduzione l'ID operatore che in quel momento sta visualizzando il filmato); i log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati)
<b><u>Quali strumenti di tracciabilità vengono utilizzati?</u></b>	<i>File di log</i> (il sistema conserva un <i>log</i> degli accessi alla consultazione delle immagini; gli operatori autorizzati alla visualizzazione delle immagini, una volta effettuato il download, sono loggati all'interno del sistema ciascuno con il proprio profilo di competenza); ogni operazione eseguita da qualsiasi utente collegato al sistema di gestione viene tracciata e registrata
<b><u>Misure anti-malware</u></b>	<i>Antivirus</i> (tutti i dispositivi pc sono dotati di antivirus costantemente aggiornato)
<b><u>Backup</u></b>	<i>Backup</i> giornaliero (i sistemi e i <i>software</i> (quindi ad esclusione dei contenuti multimediali) sono soggetti a <i>backup</i> remoto giornaliero con <i>policy</i> di <i>data retention</i> di 7 giorni necessari per finalità di <i>disaster recovery</i> )
<b><u>Sicurezza dei canali informatici</u></b>	- A protezione dell'intera architettura sono presenti i <i>firewall</i> del fornitore di <i>hosting</i> (Microsoft Azure), configurati per ammettere le sole comunicazioni

	<p>provenienti dall'esterno dell'infrastruttura virtuale (Internet / Sedi del cliente) verso i relativi servizi (HTTPS/TCP con cifratura SSL TLS 1.3 - porta TCP/433)</p> <ul style="list-style-type: none"> <li>- Il traffico avviene su canale TLS 1.3 dedicato e criptato</li> <li>- Segregazione dell'infrastruttura hardware; l'intera infrastruttura è contenuta su un gruppo risorse dedicato al cliente (Tenant) con una segmentazione in sottorete fisicamente isolata (VPC) e separata da quelle degli altri clienti</li> <li>- Internamente la soluzione viene erogata tramite orchestratori di risorse container (Kubernetes)</li> <li>- Ogni informazione viene protetta in transito da protocollo TLS 1.3 con cifrature e hashing SHA256</li> <li>- Tutte le comunicazioni con i servizi su <i>cloud</i> sono cifrate e trasferite su canale con certificato SSL</li> <li>- Aggiornamento delle <i>patch</i> di sicurezza (l'amministratore di sistema effettua interventi almeno trimestrali per allineare le versioni del software in uso con le ultime patch migliorative;</li> </ul>
--	--

	<p>provvede, inoltre, ai passaggi di versione, laddove sopraggiungano le scadenze del supporto ufficiale dei suddetti <i>software</i>)</p> <ul style="list-style-type: none"> <li>- Le connessioni amministrative privilegiate avvengono esclusivamente su canale VPN tramite protocollo SSH con chiave privata (Linux) o RDP (Windows)</li> </ul>
<b><u>Altra misura tecnica implementata</u></b>	I dati sono archiviati in <i>cloud</i> in altissima affidabilità e ridondanza fisica; bodycam e relativo <i>software</i> sono progettati per evitare manomissioni dall'esterno

## **VALUTAZIONE DEL RISCHIO RESIDUO**

Individuate ed implementate le misure di sicurezza nell'ambito del presente trattamento di dati personali, si procede alla valutazione del rischio residuo per ciascuna area (accesso, modifica, perdita), al fine di determinare se esso sia stato ridotto adeguatamente e abbia raggiunto un livello accettabile

### **ACCESSO ILLEGITTIMO**

AREA	VULNERABILITÀ	MISURE DI SICUREZZA IMPLEMENTATE
<b>ACCESSO ILLEGITTIMO</b>	<ul style="list-style-type: none"> <li>- Scattare foto dello schermo</li> </ul>	<ul style="list-style-type: none"> <li>- l'operatore che registra le immagini attraverso il dispositivo indossabile, come anche l'operatore di postazione, non hanno la possibilità di visionare le immagini, né tantomeno di modificarle in alcun modo</li> </ul>

		<ul style="list-style-type: none"> <li>- 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</li> </ul>
	<ul style="list-style-type: none"> <li>- Copia non autorizzata del contenuto</li> </ul>	<ul style="list-style-type: none"> <li>- l’applicativo implementa un sistema di <i>audit log</i> atto a registrare le attività effettuate dagli utenti e dal sistema</li> <li>- i contenuti multimediali presenti nello <i>storage</i> della camera sono cifrati con una chiave pubblica, la cui controparte privata non è presente nella camera stessa; pertanto, anche qualora si dovesse riuscire ad avere accesso ai contenuti della camera, non sarebbe possibile decifrarli per riprodurli</li> </ul>
	<ul style="list-style-type: none"> <li>- Visione delle immagini senza essere autorizzati</li> </ul>	<ul style="list-style-type: none"> <li>- gli operatori che raccolgono le immagini non possono accedervi in alcun modo (schermo oscurato)</li> <li>- il <i>cloud</i> su cui sono archiviate le immagini è accessibile solo a specifici soggetti individuati dal direttore di UOC tramite opportuna procedura operativa</li> <li>- l’accesso all’applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali</li> </ul>
	<ul style="list-style-type: none"> <li>- Recupero di un dispositivo hardware scartato</li> </ul>	<ul style="list-style-type: none"> <li>- i contenuti multimediali presenti nello <i>storage</i> della camera sono cifrati con una chiave pubblica, la cui controparte privata non è presente nella camera stessa; pertanto, anche qualora si dovesse riuscire ad avere</li> </ul>

		accesso ai contenuti della camera, non sarebbe possibile decifrarli per riprodurli
	- Sistema di autenticazione non adeguato	- Possono essere messi in atto protocolli di <i>Strong Authorization</i> - <i>cloud</i> accessibile solo al personale autorizzato; il sistema sarà connesso con l'AD dell'Amministrazione ed erediterà tutte le policy di autenticazione imposte
	- Accesso non riservato ai locali delle postazioni fisiche di controllo	- Presenza di personale all'interno delle postazioni autorizzato alla visualizzazione delle immagini provenienti dalle bodycam

All'esito della valutazione delle misure di sicurezza implementate sopra descritte, si ritiene che queste riducano significativamente le probabilità di accesso non autorizzato.

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
<div style="display: flex; flex-direction: column; align-items: flex-start;"> <div style="display: flex; align-items: center; margin-bottom: 2px;"> <div style="width: 10px; height: 10px; background-color: green; margin-right: 5px;"></div> 1, 2, 3 TRASCURABILE </div> <div style="display: flex; align-items: center; margin-bottom: 2px;"> <div style="width: 10px; height: 10px; background-color: yellow; margin-right: 5px;"></div> 4, 6, 8 LIMITATO </div> <div style="display: flex; align-items: center;"> <div style="width: 10px; height: 10px; background-color: red; margin-right: 5px;"></div> 9, 12, 16 MASSIMO </div> </div>	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

**$R_r = I(2) \times P(1) \rightarrow 2$  RISCHIO TRASCURABILE**

## **MODIFICA INDESIDERATA**

AREA	VULNERABILITÀ	MISURE DI SICUREZZA IMPLEMENTATE
<b>MODIFICA INDESIDERATA</b>	<ul style="list-style-type: none"> <li>- Errori durante gli aggiornamenti, la configurazione o manutenzione</li> </ul>	<ul style="list-style-type: none"> <li>- Aggiornamento delle <i>patch</i> di sicurezza</li> <li>- Crittografia asimmetrica (i contenuti multimediali presenti nello storage della camera sono cifrati con una chiave pubblica, la cui controparte privata non è presente nella camera stessa; pertanto, anche qualora si dovesse riuscire ad avere accesso ai contenuti della camera, non sarebbe possibile decifrarli per riprodurli)</li> </ul>
	<ul style="list-style-type: none"> <li>- Infezione da codice malevolo</li> </ul>	<ul style="list-style-type: none"> <li>- <i>Antivirus</i> (tutti i dispositivi pc sono dotati di antivirus costantemente aggiornato)</li> <li>- Sistema di sicurezza perimetrale</li> </ul>
	<ul style="list-style-type: none"> <li>- Rimozione dei componenti essenziali al corretto funzionamento</li> </ul>	<ul style="list-style-type: none"> <li>- Aggiornamento delle <i>patch</i> di sicurezza</li> </ul>
	<ul style="list-style-type: none"> <li>- Errore dell'operatore che modifica i dati</li> </ul>	<ul style="list-style-type: none"> <li>- Attività di <i>logging</i> volta a verificare le modifiche indesiderate</li> <li>- Presenza di un sistema di <i>backup</i></li> <li>- Formazione del personale</li> </ul>
	<ul style="list-style-type: none"> <li>- Scarse competenze</li> </ul>	<ul style="list-style-type: none"> <li>- Formazione del personale</li> </ul>

All'esito della valutazione delle misure di sicurezza implementate sopra descritte, si ritiene che queste riducano significativamente le probabilità di modifica indesiderata.



ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
<div>■ 1, 2, 3 TRASCURABILE</div> <div>■ 4, 6, 8 LIMITATO</div> <div>■ 9, 12, 16 MASSIMO</div>	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)

**$R_r = I(1) \times P(1) \rightarrow 1$  RISCHIO TRASCURABILE**

\*\*\*

## **PERDITA ACCIDENTALE**

AREA	VULNERABILITÀ	MISURE DI SICUREZZA IMPLEMENTATE
<b>MODIFICA INDESIDERATA</b>	- Interruzione di corrente	- <i>Backup</i> giornaliero (i sistemi e i <i>software</i> (quindi ad esclusione dei contenuti multimediali) sono soggetti a <i>backup</i> remoto giornaliero con policy di <i>data retention</i> di 7 giorni necessari per finalità di <i>disaster recovery</i> )
	- Surriscaldamento eccessivo	- Come sopra
	- Attacco informatico	- <i>Antivirus</i> (tutti i dispositivi sono dotati di antivirus costantemente aggiornato - Sistema di sicurezza perimetrale

	<ul style="list-style-type: none"> <li>- Inondazioni, incendi, atti vandalici, danni naturali, usura, malfunzionamento del dispositivo</li> </ul>	<ul style="list-style-type: none"> <li>- Sistema di <i>backup</i></li> </ul>
	<ul style="list-style-type: none"> <li>- Errori del personale che accidentalmente cancella i dati</li> </ul>	<ul style="list-style-type: none"> <li>- Formazione del personale</li> </ul>
	<ul style="list-style-type: none"> <li>- Errore durante gli aggiornamenti</li> </ul>	<ul style="list-style-type: none"> <li>- Aggiornamento delle <i>patch</i> di sicurezza</li> <li>- Formazione del personale</li> </ul>

All'esito della valutazione delle misure di sicurezza implementate sopra descritte, si ritiene che queste riducano significativamente le probabilità di perdita accidentale.

ALTAMENTE PROBABILE (4)	4	8	12	16
PROBABILE (3)	3	6	9	12
POCO PROBABILE (2)	2	4	6	8
IMPROBABILE (1)	1	2	3	4
<div style="display: flex; align-items: center;"> <div style="width: 10px; height: 10px; background-color: green; margin-right: 5px;"></div> 1, 2, 3 TRASCURABILE  <div style="width: 10px; height: 10px; background-color: yellow; margin-right: 5px; margin-top: 2px;"></div> 4, 6, 8 LIMITATO  <div style="width: 10px; height: 10px; background-color: red; margin-right: 5px; margin-top: 2px;"></div> 9, 12, 16 MASSIMO </div>	LIEVE (1)	MEDIO (2)	GRAVE (3)	GRAVISSIMO (4)


**$R_r = I (2) \times P (1) \rightarrow 2$  RISCHIO TRASCURABILE**

## VALUTAZIONE DEL RISCHIO RESIDUO

AREE DI RISCHIO	STIMA IMPATTO	STIMA PROBABILITA'
RISERVATEZZA	MEDIO	IMPROBABILE
INTEGRITA'	LIEVE	IMPROBABILE
DISPONIBILITA'	MEDIO	IMPROBABILE
VALUTAZIONE (si prende in considerazione il valore più alto tra le valutazioni riferite alle voci RID)	2	1

## CALCOLO DEL RISCHIO RESIDUO DEL TRATTAMENTO

$$R_r = I (2) \times P (1) \rightarrow 2 \text{ RISCHIO TRASCURABILE}$$

	<b>TRASCURABILE</b>	Combina bassa probabilità e basso impatto
	<b>LIMITATO</b>	Combina probabilità e impatto moderati
	<b>SIGNIFICATIVO</b>	Combina alta probabilità e impatti significativi
	<b>MASSIMO</b>	Combina probabilità massima e impatti critici

A seguito dell'applicazione delle misure di sicurezza tecniche e organizzative, il rischio inerente, inizialmente calcolato, è risultato opportunamente mitigato, portando ad un livello di rischio residuo del trattamento in questione che si ritiene:

ACCETTABILE	<input checked="" type="checkbox"/>	NON ACCETTABILE	<input type="checkbox"/>
-------------	-------------------------------------	-----------------	--------------------------

# PARERE DEL DPO

NOME DEL DPO	Scudo Privacy S.r.l., nella persona dell'Avv. Sarah Masato
PARERE DEL DPO	<p>In virtù delle misure tecnico-organizzative previste nell'ambito del presente trattamento di dati personali, si ritiene che il rischio residuo possa essere accettato dal Titolare del Trattamento. Si raccomanda di monitorare e verificare periodicamente l'efficacia delle misure di sicurezza applicate e di garantire la revisione delle politiche di revisione dei dati, ivi compresa un'adeguata formazione del personale coinvolto in tale attività trattamentale.</p> <p>Il DPO si riserva di sorvegliare lo svolgimento del riesame periodico della Valutazione d'Impatto condotta, al fine di garantire la conformità al GDPR e al Codice Privacy.</p>
VALUTAZIONE	<ul style="list-style-type: none"><li>■ Accettabile</li><li>□ Migliorabile</li><li>□ Da correggere</li></ul>

DATA

FIRMA LEGALE RAPP. TE