SEDE LEGALE
via Curtatone, 54 - 52100 AREZZO
Centralino: 0575 2551
P.I. e C.F.: 02236310518
web: www.uslsudest.toscana.it
pec: ausltoscanasudest@postacert.toscana.it

SEDI OPERATIVE
SIENA - Piazza Carlo Rosselli, 26 - Centralino: 0577.535111
GROSSETO - Via Cimabue, 109 - Centralino: 0564.485111
AREZZO - Via Curtatone, 54 - Centralino: 0575.2551

Valutazione d'impatto sulla protezione dei dati

ai sensi dell'art. 35 Regolamento (UE) 679/2016 (RGPD)

	Nome e Cognome	*Telefono*	*Email*	*Struttura organizzativa*	*Sede*
Preposto al trattamento	Direttore del Presidio Ospedaliero	0577994722			PO Alta Val D'Elsa
Referente per la redazione	Dr Santoriello Giancarlo Bartoli Stefano	0577994392 0577994710	giancarlo.santoriello@uslsudest.toscana.it; stefano.bartoli@uslsudest.toscana.it;	UOC DMPO AVDE UOC Manutenzioni Area P. Senese	PO Alta Val D'Elsa PO Alta V'Elsa

SOMMARIO

1. CONTESTO

1.1 Denominazione del trattamento
1.2 Breve descrizione del trattamento
1.3 Finalità e base giuridica del trattamento
1.4 Descrizione dell'intero ciclo del trattamento
1.5 RESPONSABILITÀ CONNESSE AL TRATTAMENTO
1.5.1 Soggetti interni che partecipano al trattamento
1.5.2 Soggetti esterni che partecipano al trattamento
1.6 Dati trattati
1.7 Standard applicabili al trattamento
1.8 Dove sono fisicamente allocati i dati

2. PRINCIPI FONDAMENTALI

2.1 PROPORZIONALITÀ E NECESSITÀ

2.1.1 Perché vi è necessità di utilizzare questo sistema/trattamento?
2.1.2 Gli scopi del trattamento sono specifici, espliciti e legittimi?
2.1.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? I dati raccolti sono solo i dati necessari alle finalità del trattamento?
2.1.4 I dati sono esatti e aggiornati? In quale modo sono aggiornati?
2.1.5 I dati sono trasferiti? Come sono trasferiti?

2.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

2.2.1 Come sono informati del trattamento gli interessati?
2.2.2 Ove applicabile: come si ottiene il consenso degli interessati?
2.2.3 Come possono gli interessati esercitare il loro diritto di accesso (Sezione 2, art. 15 RGPD)?
2.2.4 Come possono gli interessati esercitare i loro diritti di rettifica, cancellazione, limitazione del trattamento e alla portabilità dei dati (Sezione 3, artt. 16, 17, 18, 20 RGPD)?
2.2.5 Come possono gli interessati esercitare il loro diritto di opposizione (Sezione 4, art. 21

RGPD)?
2.2.6 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente? Oppure devono essere attuate misure supplementari perché siano rispettate le garanzie essenziali?

3. RISCHI

3.1 RISCHIO POTENZIALE INIZIALE

3.1.1 Valutazione dell'impatto
3.1.2 Valutazione della probabilità
3.1.3 Individuazione delle fonti di rischio
3.1.4 Valutazioni (iniziali) di impatto e probabilità complessive
3.1.5 Valutazione del rischio iniziale

3.2 MISURE ESISTENTI O PIANIFICATE

3.3 RISCHIO RESIDUO STIMATO

3.3.1 Rivalutazioni di impatto e probabilità complessive
3.3.2 Rivalutazione del rischio

4. PIANO DI TRATTAMENTO RISCHIO RESIDUO

---

1. CONTESTO

1.1

1.1 TITOLO
Installazione delle apparecchiature di videosorveglianza presso la sede operativa P.O. ALTA VAL D'ELSA loc. Campostaggia nel Comune di Poggibonsi (SI) area del PRONTO SOCCORSO;

Denominazione del trattamento:
Gestione impianto di videosorveglianza con registrazione immagini, accesso alle immagini registrate, eventuale copia delle immagini registrate nei casi strettamente necessari e previsti dalla legge, eventuale trasmissione delle immagini su richiesta dell'autorità giudiziaria, cancellazione delle immagini.

1.2 Breve descrizione del trattamento *(finalità, risultati attesi, contesto di utilizzo...)*

Le aggressioni al personale sanitario sono riconosciute dall'OMS come un importante problema di salute pubblica. E' un fenomeno che può presentarsi in modi diversi: dall'aggressione alle minacce, potendo arrivare alla violenza fisica, fino ad un possibile epilogo più estremo come l'omicidio.
Il fenomeno ha un'importanza rilevante ed attualmente in crescita, tanto che può essere considerato una vera e propria emergenza sociale, anche a causa di un atteggiamento culturale e di pregiudizi nei confronti del personale sanitario, ritenuto responsabile di attese, ritardi e di presunta malasanità.
Il problema non è conosciuto nella sua reale dimensione, a causa della scarsa propensione alla segnalazione degli eventi accaduti, tuttavia, per quanto noto, sappiamo che in ambito sanitario la percentuale di infortuni riferibili ad aggressione, rispetto agli infortuni denunciati, è decisamente superiore rispetto ad altri comparti lavorativi. Il dato è da ritenersi significativo ed è verosimilmente ascrivibile al rapporto fortemente interattivo e personale che si instaura tra personale sanitario e pazienti-familiari, i quali possono trovarsi talvolta in una condizione di particolare vulnerabilità, frustrazione e stress emotivo.
Il rischio di subire aggressione sul posto di lavoro deve essere considerato al pari di ogni altro rischio lavorativo (D.Lgs81/2008 e s.m.i.) ma a differenza di altri rischi lavorativi quelli correlati ad aggressione sono caratterizzati da estrema variabilità e imprevedibilità.
Peraltro data la sua crescente rilevanza è necessario considerare il problema non solo in relazione alla sicurezza del lavoratore in senso stretto ma come un fenomeno che, andando a minare le condizioni di lavoro e il benessere degli operatori sanitari, si ripercuote sulla qualità delle prestazioni erogate e in ultima analisi sulla la sicurezza delle cure.
Tra i Servizi maggiormente coinvolti dai rapporti del Ministero della Salute, 2007 ci sarebbero proprio i Servizi di Emergenza ed Urgenza tra i quali i Pronto Soccorso ed in particolar modo le aree di attesa e triage.
In linea con il dato nazionale si è visto nell'ultimo anno incremento delle segnalazioni di aggressioni agli operatori anche nel Pronto Soccorso della Val D'Elsa, nonostante negli ultimi anni fossero state intraprese ulteriori misure organizzative fra cui un Servizio di Sorveglianza notturna mobile nell'ospedale con prevalente postazione presso il Pronto soccorso, dalle ore 20 alle ore 7 di mattina 7 giorni 7. Ma la non continuità ed esclusività del servizio ha fatto nascere la necessità di valutare un sistema di videosorveglianza senza operatore, mediante videoregistrazione, attraverso telecamere posizionate nell'area di accesso esterne al pronto soccorso ed in quelle di attesa interne allo stesso.

1.3 Base giuridica del trattamento

- (**x) Art. 6 RGPD - paragrafo 1 lett. c);**
- (**x) Art. 6 RGPD - paragrafo 1 lett. e);**
- **(x) Art. 9 RGPD - paragrafo 2 lett.g;**
- **(x) Art. 2-sexies D.lgs. 196/2003 - comma 2, lett. u);**
- **(X) Art. 2-septies D.lgs. 196/2003;**
- **(X) Art. 10 RGPD;**
- **Il Provvedimento Generale in tema di Videosorveglianza 8 aprile 2010;**
- **Lo Statuto dei Lavoratori (art. 4 Legge n. 300/1970);**
- **Le Linee Guida n. 3/2019 dell'EDPB (Comitato dei Garanti Europeo)**
- **Legge n. 113 del 14 agosto 2020** *"Disposizioni in materia di sicurezza per gli esercenti le professioni sanitarie e socio-sanitarie nell'esercizio delle loro funzioni";*
- **Delibera Giunta Regione Toscana n. 1183 del 16/10/2023 "***progetto prevenzione delle aggressioni al personale sanitario e socio-sanitario;*

1.4 Descrizione dell'intero ciclo del trattamento *(descrivere il ciclo di vita dei dati, fornendo una dettagliata descrizione di ciascun processo effettuato – es. raccolta, elaborazione, conservazione, etc. - e specificando le risorse che ospitano i dati oggetto del trattamento, come sistemi operativi, server, software, reti, supporti cartacei, etc.)*

Le telecamere di Videosorveglianza saranno posizionate nelle zone a maggior rischio: sale attesa utenti, triage e pretriage, come meglio specificati nella planimetria allegata (doc. n. 1) e sono necessari per garantire sia la sicurezza degli utenti e dei lavoratori oltre che la tutela del patrimonio aziendale.

L'impianto sarà costituito da complessive n.9 telecamere e da n. 1 unità di registrazione **e** consente la registrazione ed eventuale visione in differita delle immagini (DVR); esso è dotato di hard disk 1Tb, conforme alle normative sulla privacy e composto da software protetto da password personale per ogni soggetto autorizzato al trattamento.

L'unità di registrazione sarà installata all'interno di ufficio del Pronto soccorso, all'interno di un ulteriore box /armadio con chiusura a chiave. Quest'ultima sarà nella disponibilità del solo personale autorizzato.

Le immagini riprese dalle telecamere sono registrate su di unità Hard Disk, e sono conservate per un periodo di 72 ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione su richiesta motivata del preposto al trattamento (fino a un massimo di 96 ore) nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria, dopo di ché le immagini si sovrapporranno alle precedenti, cancellandole automaticamente. Le immagini potranno essere visionate solo dal personale, incaricato e precedentemente autorizzato, sulla unità di visione

1.5 RESPONSABILITÀ CONNESSE AL TRATTAMENTO

1.5.1 Soggetti interni che partecipano al trattamento *(indicare i soggetti che partecipano al trattamento e il relativo ambito di responsabilità)*

ll Titolare del trattamento, dei dati raccolti con i sistemi di videosorveglianza, è l'Azienda U.S.L. Toscana sud est, nella persona del suo Direttore Generale.

Il Preposto al trattamento per la gestione dati del sistema di videosorveglianza è il Direttore P.O. Alta val D'Elsa: che ha l'obbligo di verificare che le operazioni di utilizzo e trattamento dei dati visivi siano svolte esclusivamente per gli scopi precedentemente descritti.

Il Preposto può designare per iscritto i soggetti " Incaricati " al trattamento e gestione dei dati i quali, operano sotto la sua diretta autorità.

Gli incaricati al trattamento sono figure autorizzate all'accesso ai locali, all'armadio dove è presente l'unità di memoria ed alla visione e gestione delle immagini.

1.5.2 Soggetti esterni che partecipano al trattamento:

E'nominata "**responsabile ex art 28 GDPR"** la ditta esterna che provvede alla manutenzione dell'impianto**,** e che deve individuare formalmente i propri dipendenti incaricati al trattamento.

1.6 Dati trattati *(elencare i dati in dettaglio e non con generico rimando alla tipologia - ad esempio: non usare solo*

l'espressione "dati anagrafici", ma specificare se: nome, cognome, data nascita, luogo nascita, C.F., numero tessera sanitaria; per i dati contatto specificare se: indirizzo di posta elettronica, PEC, indirizzo mail istituzionale, numero di telefono fisso e mobile,). Specificare anche la tipologia di interessati cui si riferiscono i dati, ad esempio: pazienti, familiari del paziente, dipendenti, collaboratori, etc.)
Consisteranno in immagini digitali di utenti, accompagnatori, personale sanitario e socio sanitario, registrate h24 e conservate per 72. Allo scadere delle del tempo indicato, le immagini saranno cancellate automaticamente; Alla ditta installatrice saranno impartite precise indicazioni circa il puntamento delle stesse direttamente dal preposto al trattamento anche attraverso le strutture tecniche interne al Presidio Ospedaliero, al fine di garantire il principio di minimizzazione) Le telecamere che saranno installate potranno incidentalmente riprendere i lavoratori dell'AziendaUsl Toscana sud est e per questo motivo ai sensi dell'art.4 della Legge n.300/1970 e s.m.i. Statuto dei Lavoratori si procederà alla sottoscrizione di specifico accordo con le Organizzazioni Sindacali.
1.7 Standard applicabili al trattamento *(esempi: codici di condotta ex art. 40 RGPD, regole deontologiche, altre misure di garanzia (v. misure adottate dal Garante per la protezione dei dati personali), altri meccanismi di certificazione (v. standard UNI-ISO in materia di sistemi informatici), procedure/protocolli o altra regolamentazione aziendale,...*
Disposizioni regolamentari in materia di videosorveglianza dei tre ambiti provinciali confluiti nell'azienda Usl Toscana sud est; è in corso di predisposizione il regolamento di AUTSE:
1.8 Dove sono fisicamente allocati i dati
Le immagini riprese dalle telecamere verranno registrate su unità Hard Disk di registrazione che le conserverà per 72 ore dalla registrazione, dopo di ché le immagini si sovrapporranno alle precedenti, cancellandole, fatte salve speciali esigenze di ulteriore conservazione su richiesta motivata del preposto, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria. L'unità di Registrazione sarà installata all'interno di ufficio del Pronto soccorso, all'interno di un ulteriore box /armadio con chiusura a chiave. Le chiavi del locale dove verrà collocato il VDR e le chiavi dell'armadio protetto saranno fornite al solo personale autorizzato, unitamente alle password per accedere all'unità di registrazione.,

2. PRINCIPI FONDAMENTALI

2.1 PROPORZIONALITÀ E NECESSITÀ

N.B. La finalità del trattamento dei dati deve essere definita prima di iniziare il trattamento necessario a perseguire una finalità legittima, specifica e definita (per scopi ulteriori solo se specifici e compatibili con la finalità iniziale). I dati personali devono essere trattati solo se la finalità non è ragionevolmente conseguibile con altri mezzi. Il trattamento dei dati non deve interferire in modo sproporzionato con gli interessi, i diritti e le libertà in gioco.

2.1.1 Perché vi è necessità di utilizzare questo sistema/trattamento?
Risposta: Il Pronto soccorso di Campostaggia è dall'inizio delle sua attività (anno 2000) privo di un presidio fisso di polizia/carabinieri. Questo ha fatto si che negli ultimi due anni, in seguito ai primi episodi di aggressione, sia stato adottato un Servizio di sorveglianza privata di guardie giurate notturne, dedicato però a tutta l'area ospedaliera dislocata su più piani. Avendo riscontrato i primi episodi di aggressione nell'area del Pronto Soccorso, in particolare 31 aggressioni censiti nel 2024 mentre nel 2023 sono stati solo 3 (dati del SPP USL SUDEST), è stato ritenuto necessario attenzionare maggiormente l'area sopra indicata in maniera più completa ed incisiva. La soluzione più opportuna è stata l'adozione di un sistema di videosorveglianza continuo e senza operatore.
2.1.2 Gli scopi del trattamento sono specifici, espliciti e legittimi?
Per L'Azienda Sanitaria, è un dovere garantire l'assolvimento dei compiti istituzionali tra cui quelli a garanzia della sicurezza del proprio personale, nonchè di coloro che accedono alle strutture aziendali, adottando tutte le attività e misure precauzionali oltre a sistemi di deterrenza. La realizzazione di un nuovo impianto di videoregistrazione inoltre, permette la salvaguardia del proprio patrimonio e dei propri immobili, oltre che l'individuazione di eventuali comportamenti violenti che possono mettere a repentaglio la sicurezza del personale sanitario e degli stessi utenti. I dati personali raccolti per le suddette finalità non possono essere utilizzati per finalità diverse o ulteriori, salvo le esigenze di polizia giudiziaria e non possono essere diffusi o comunicati a terzi non legittimati.
2.1.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? I dati raccolti sono solo i dati necessari alle finalità del trattamento?

Risposta:
Le telecamere sono a ripresa fissa e non hanno la funzione di "zoom" dell'area di oggetto di ripresa. L'angolo di ripresa e la panoramica di ripresa vengono definiti per ogni telecamera in modo tale da limitare l'angolo di visuale e sono posizionate in modo da raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, evitando (quando non indispensabile) immagini dettagliate. Le telecamere di videosorveglianza sono installate nel rispetto del divieto di controllo a distanza dell'attività dei lavoratori (applicazione di filtri e oscuramento ove necessario).
II trattamento dei dati, rilevati attraverso il sistema di telecamere a circuito chiuso, avviene secondo correttezza e per scopi determinati e legittimi, ed in applicazione del divieto di controllo a distanza dei lavoratori di cui all'art. 4 c.1 lettera della L.300/1970, nel rispetto delle disposizioni contenute nel D.Lgs. 30 Giugno 2003 n. 196, e dal Regolamento UE 679/2016 Regolamento generale sulla Protezione dei Dati RGPD.
Inoltre le telecamere non sono dotate di sistemi di rilevazione sonora che possono configurare ipotesi di intercettazione di comunicazione e/o conversazioni.
Le telecamere sono collocate nei luoghi in cui altre misure (es. sistemi di allarme, controlli fisici o logistici, misure di protezione degli ingressi) non sono sufficienti a perseguire le finalità dichiarate. Per le finalità di protezione delle persone e tutela dei beni sopra specificate, le telecamere sono collocate esclusivamente presso zone soggette a concreti pericoli o per le quali ricorra un'effettiva esigenza di deterrenza. L'attività di videosorveglianza è svolta nel rispetto del principio di proporzionalità nella scelta delle modalità di ripresa e di dislocazione degli impianti. L'angolo di ripresa e la panoramica di ripresa vengono definiti per ogni telecamera in modo tale da limitare l'angolo di visuale e sono posizionate in modo da raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, evitando (quando non indispensabile) immagini dettagliate.
La chiara segnalazione delle postazioni delle unità di ripresa, la conservazione dei dati nel solo dispositivo di registrazione c/o locale ad accesso limitato ed all'interno di un box/armadio chiuso a chiave sono alcuni elementi che caratterizzano la raccolta dati per le sole finalità indicate in premessa. Inoltre, l'eventuale scaricamento dei dati da parte dei pochi autorizzati per un lasso di tempo (tracciato e determinato) strettamente necessario per conseguire gli scopi per cui sono raccolti e solo in seguito ad esplicita richiesta delle autorità, ulteriori accorgimenti tecnici informatici come le tecniche di solarizzazione dei dipendenti e la scarsa definizione delle riprese, consentono ai soli autorizzati di mettere a disposizione immagini riconoscibili alle sole autorità intervenenti sul momento, adempiono al rispetto dei principi di cui all'art. 5 paragr. 1 lett. c) RGPT;
.In caso di accesso dell'interessato , questi può avere accesso alle sole immagini che lo riguardano direttamente, mediante la schermatura (anche manuale), se necessaria, delle immagini del video che riprendano soggetti terzi; la visione può comprendere eventuali dati riferiti a terzi nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali dell'interessato. Nel caso di richiesta di duplicazione di immagini registrate in cui compaiano soggetti terzi, deve essere utilizzato apposito programma oscuratore.

2.1.4 I dati sono esatti e aggiornati? In quale modo sono aggiornati?

Risposta:
La sovrascrittura automatica dei dati prevista rende inapplicabile l'aggiornamento;

2.1.5 I dati sono trasferiti? Come sono trasferiti?

Risposta: Risulta impossibile un trasferimento fuori dalla struttura fisica dell'ospedale, non essendo immessi in alcuna rete interna (intranet) ed esterna (internet); Inoltre risulta ulteriormente impossibile un'estrazione dei dati fuori dalle legittime richieste degli interessati o dell'Autorità Giudiziaria.

I dati sono trasferiti fuori dell'Azienda? *(Selezionare la voce che interessa apponendo una X tra le parentesi)*		
SI ( )	**NO (X)**	**NON SO ( )**
I dati sono trasferiti fuori dell'Italia?		
SI ( )	**NO (X)**	**NON SO ( )**
I dati sono trasferiti fuori dello Spazio Economico Europeo? (SEE, ossia UE + Norvegia, Liechtenstein, Islanda)		
SI ( )	**NO (X)**	**NON SO ( )**

2.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

2.2.1 Come sono informati del trattamento gli interessati?

Risposta:
Tutti coloro che accedono alla struttura ed alle aree dove sono installate le telecamere saranno opportunamente informati, mediante specifica segnaletica dell'esistenza di impianti di videosorveglianza nell'area in cui stanno per accedere/transitare;

I cartelli di "avviso" saranno collocati prima del raggio di azione delle videocamere, anche nelle sue immediate vicinanze, in modo tale che i soggetti interessati comprendano, prima di accedervi, di essere all'interno di un'area videosorvegliata, avranno dimensioni e caratteri alfabetici tali da essere chiaramente visibili anche in condizioni di scarsa od insufficiente illuminazione, riporteranno indicazioni o simboli per precisare che le riprese saranno registrate.
Sul sito Internet aziendale è pubblicato il testo completo dell'informativa.

2.2.2 Ove applicabile: come si ottiene il consenso degli interessati?

Risposta: non applicabile

2.2.3 Come possono gli interessati esercitare il loro diritto di accesso (art. 15 RGPD)?

Risposta:

Il soggetto interessato può richiedere l'accesso alle registrazioni che lo riguardano presentando una istanza al Titolare o al Responsabile della Protezione dati personali, i cui dati di contatto sono riportati nell'informativa di primo e secondo livello, o al preposto al trattamento (Direttore Presidio) dei dati dell'impianto che ha effettuato le registrazioni entro il termine previsto per la conservazione delle immagini. L'istanza deve essere presentata in forma scritta e deve contenere gli elementi atti a circoscrivere l'oggetto della richiesta sia sotto il profilo spaziale che temporale. Può essere utilizzato anche il modulo pubblicato nel sito web aziendale al seguente indirizzo: www.uslsudest.toscana.it/images/azienda/privacy/documentazione/diritto-protezione_dati_0451.pdf

Nel caso che le immagini di possibile interesse non siano più conservate, sarà data formale comunicazione al richiedente.

2.2.4 Come possono gli interessati esercitare i loro diritti di rettifica, cancellazione, limitazione del trattamento e alla portabilità dei dati (artt. 16, 17, 18, 20 RGPD)?

Risposta:

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. Nel caso di specie, trattandosi di trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri il diritto alla portabilità non si applica.

Per l'esercizio del diritto alla cancellazione ed alla limitazione del trattamento il soggetto interessato può presentare una istanza al Titolare o al Responsabile della Protezione dati personali, i cui dati di contatto sono riportati nell'informativa di primo e secondo livello, anche utilizzando il modulo pubblicato nel sito web aziendale al seguente indirizzo: www.uslsudest.toscana.it/images/azienda/privacy/documentazione/diritto-protezione_dati_0451.pdf

2.2.5 Come possono gli interessati esercitare il loro diritto di opposizione (art. 21 RGPD)?

Risposta:

Il soggetto interessato può presentare una istanza al Titolare o al Responsabile della Protezione dati personali, i cui dati di contatto sono riportati nell'informativa di primo e secondo livello, anche utilizzando modulo pubblicato nel sito web aziendale al seguente indirizzo www.uslsudest.toscana.it/images/azienda/privacy/documentazione/diritto-protezione_dati_0451.pdf

2.2.6 In caso di trasferimento di dati al di fuori dello Spazio Economico Europeo, i dati godono di una protezione equivalente? Oppure devono essere attuate misure supplementari perché siano rispettate le garanzie essenziali?

Risposta*:* E' esclusa tale possibilità in quanto si tratta di un circuito chiuso.

3. RISCHI

3.1 RISCHIO POTENZIALE INIZIALE

Il livello di **rischio** è determinato dal prodotto della **probabilità di accadimento** di un evento/minaccia per **il potenziale impatto** su diritti e libertà degli interessati esercitato da tale evento qualora si verifichi.
Primariamente occorre procedere ad una valutazione del **rischio potenziale inizialmente valutato senza i controlli e le misure di sicurezza applicate.** Tale valutazione corrisponde al prodotto dei valori associati alla valutazione dell'**IMPATTO** e della **PROBABILITÀ**, stimati secondo le scale di seguito esposte.

3.1.1 VALUTAZIONE DELL'IMPATTO

L'**IMPATTO** è classificato secondo una scala da 1 a 5.

IMPATTO	**5**	**Grave**	*Gli interessati possono avere conseguenze significative, o addirittura irreversibili, che non possono superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte,…).*
	4	**Significativo**	*Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare, anche se con gravi difficoltà (perdita significativa di denaro, inserimento di liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute,…).*
	3	**Importante**	*Gli interessati possono incontrare significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici minori,…).*
	2	**Limitato**	*Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema (perdita di tempo per reinserire informazioni, fastidio, irritazioni,…).*
	1	**Trascurabile**	*Gli interessati non incontrano inconvenienti significativi.*

L'impatto dovrà essere stimato in rapporto alle eventualità di **ACCESSO ILLEGITTIMO DI DATI** (collegato al rischio di **perdita di riservatezza**), **MODIFICHE INDESIDERATE DEI DATI** (collegato al rischio di **perdita di integrità**) e **PERDITA DI DATI** (collegato al rischio di **mancanza di disponibilità**
La stima dell'impatto, declinata secondo i tre ambiti sopra descritti, prenderà come riferimento il valore più alto tra quelli relativi ad essi riferiti.

3.1.2 VALUTAZIONE DELLA PROBABILITÀ

La **PROBABILITÀ** è valutata su di una scala da 1 a 4 (come di seguito descritta) in base alla ipotetica probabilità/frequenza di accadimento di una minaccia, tenuto conto delle caratteristiche delle risorse che ospitano i dati oggetto di trattamento e in assenza di contromisure/controlli.

PROBABILITÀ Livello in base alla ipotetica probabilità che una minaccia si avveri ed alla sua frequenza di accadimento			
1 - Trascurabile	**2 – Limitata**	**3 - Significativa**	**4 - Massima**
Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui	*Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato*	*Appare possibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in uffici dell'organizzazione ove l'accesso è controllato da un*	*Appare estremamente facile per le fonti di rischio considerate concretizzare una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione*

accesso è controllato tramite badge e codice d'ingresso).	*tramite badge).*	*incaricato all'ingresso*	*pubblicamente accessibile)*

Anche la probabilità dovrà essere stimato in rapporto alle eventualità di **ACCESSO ILLEGITTIMO DI DATI**, **MODIFICHE INDESIDERATE DEI DATI** e **PERDITA DI DATI.**
La stima della probabilità, declinata secondo i tre ambiti sopra descritti, prenderà come riferimento il valore più alto tra quelli relativi ad essi riferiti.

3.1.3 INDIVIDUAZIONE DELLE FONTI DI RISCHIO

Devono essere individuate le fonti di rischio riferite alle tre eventualità di ACCESSO ILLEGITTIMO DI DATI, MODIFICHE INDESIDERATE DEI DATI e PERDITA DI DATI, rispetto alle quali si fornisce una mappatura dei possibili rischi.

A - Rischi in grado di portare ad un ACCESSO ILLEGITTIMO AI DATI PERSONALI			
RISCHI POSSIBILI DI FONTE UMANA E NON UMANA *(seleziona i possibili rischi o individuane ulteriori)*			
Seleziona eventuali voci di interesse	**Esempi di possibili rischi di fonte umana:**	**Seleziona eventuali voci di interesse**	**Esempi di possibili rischi di fonte strumentale (non umana):**
( )	*replica dei dati su supporto non sicuro/adatto*	**( )**	*infezioni da virus/malware*
( )	*installazione di software non autorizzato sulla postazione di lavoro*	**( )**	*sistema di autenticazione/profilazione/gestione delle credenziali non adeguato*
( )	*divulgazione involontaria delle informazioni (es in un dialogo)*	**( )**	*errori/vulnerabilità nel software utilizzato*
( )	*attacco per carpire informazioni/furto identità*	**( )**	*trasmissioni di dati in maniera non sicura*
( )	*cambio mansione, dimissioni di dipendente*	**( )**	*altro... (specificare)*
( )	*affidamento di attività di progetto/servizio a fornitori*		
(X)	*comportamenti sleali o fraudolenti di dipendenti*		
(X)	*furto di dispositivi (pc, telefono, hw…)*		
( )	*errori in fase di aggiornamento dei SO, del middleware, delle configurazioni*		
( )	*altro... (specificare)*		

Seleziona eventuali voci di interesse	***Esempi concreti:***
(X)	*scattare foto dello schermo*
(X)	*copia non autorizzata del contenuto*
(X)	*guardare lo schermo senza essere autorizzati*
( )	*recupero di un dispositivo hardware scartato*
( )	*scarto d'archivio*
(X)	*sistema di autenticazione/profilazione/gestione delle credenziali non adeguato*
(X)	*cancellazione di log*
( )	*abuso della funzione di rete*
( )	*raccolta di dati di configurazione*
( )	*installazione di uno strumento di amministrazione remota*
( )	*sostituzione di componenti durante un aggiornamento, una manutenzione o installazione*
(X)	*divulgazione involontaria di informazioni*
( )	*altro... (specificare)*

B - Rischi in grado di portare ad una MODIFICA INDESIDERATA DEI DATI PERSONALI			
RISCHI POSSIBILI DI FONTE UMANA E NON UMANA *(seleziona i possibili rischi o individuane ulteriori)*			
Seleziona eventuali voci di interesse	**Esempi di possibili rischi di fonte umana:**	**Seleziona eventuali voci di interesse**	**Esempi di possibili rischi di fonte strumentale (non umana):**
(X)	*errori umani involontari di dipendenti (es. per poca formazione/competenza, disattenzione,...)*	**( )**	*infezioni da virus/malware*
( )	*altro... (specificare)*	**( )**	*errori/vulnerabilità nel software utilizzato*
		( )	*installazione di un middleware, software o hardware che danneggia i dati*
		(X)	*errori in fase di aggiornamento dei software operativi, del middleware, delle configurazioni*
		( )	*altro... (specificare)*
Seleziona eventuali voci di interesse	***Esempi concreti:***		
( )	*aggiunta di hardware incompatibile causando malfunzionamenti*		
( )	*rimozione dei componenti essenziali al corretto funzionamento*		
(X)	*modifiche indesiderate dei dati nei data base*		
( )	*cancellazione dei file necessari per l'esecuzione del software*		
(X)	*errore dell'operatore che modifica i dati*		
( )	*errori durante gli aggiornamenti, la configurazione o manutenzione*		
( )	*infezione da codice dannoso*		
( )	*carico di lavoro elevato, stress o cambiamenti negativi delle condizioni di lavoro*		
( )	*scarse competenze*		
( )	*insufficiente capacità di svolgere i compiti assegnati*		
( )	*altro... (specificare)*		

C - Rischi in grado di portare ad una PERDITA DEI DATI			
RISCHI POSSIBILI DI FONTE UMANA E NON UMANA *(seleziona i possibili rischi o individuane ulteriori)*			
Seleziona eventuali voci di interesse	**Esempi di possibili rischi di fonte umana:**	**Seleziona eventuali voci di interesse**	**Possibili eventi relativi al contesto (eventi accidentali e eventi climatici):**
(X)	*replica dei dati su supporto non sicuro/adatto*	**(X)**	*evento naturale catastrofico (incendio, inondazione)*
(X)	*errori in fase di aggiornamento dei SO, del middleware, delle configurazioni*	**( )**	*interruzioni o non disponibilità della rete (guasti)*

(X)	*errori umani involontari di dipendenti (es per poca formazione/competenza, disattenzione,..)*	(X)	*interruzioni o non disponibilità dei sistemi complementari (elettricità, climatizzazione, ecc.)*
(X)	*evento vandalico*	( )	*altro...*
(X)	*furto di dispositivi (pc, telefono, hw)*	( )	
( )	*utilizzo di software contraffatto*	( )	**Possibili rischi di fonte strumentale (non umana):**
( )	*dimensionamento non corretto dei repository dei dati (database, file system)*	( )	*infezioni da virus/malware*
( )	*errori in fase di aggiornamento dei software applicativi*	( )	*errori/vulnerabilità nel software utilizzato*
( )	*scadenza licenza*	( )	*errori in fase di aggiornamento dei software operativi, delle configurazioni*
(X)	*indisponibilità del personale (malattia, sciopero, pensionamento, ..)*	(X)	*guasto hardware*
( )	*attacchi informatici*	( )	*altro...*
( )	*furto documenti cartacei*		
( )	*altro...*		

Seleziona eventuali voci di interesse	***Esempi concreti:***
( )	*Unità di memoria piena /superamento delle dimensioni del data base*
(X)	*interruzione di corrente*
( )	*surriscaldamento eccessivo*
( )	*attacco informatico per impedire l'uso delle risorse di sistema*
( )	*aggiunta di hardware incompatibile*
(X)	*inondazioni, incendi, atti vandalici, danni naturali usura, malfunzionamento del dispositivo*
(X)	*errori dell'operatore che cancellano i dati*
(X)	*errore durante aggiornamenti, configurazioni*
( )	*carico di lavoro elevato, stress o cambiamenti negativi delle condizioni di lavoro*
( )	*altro... (specificare)*

Alla luce delle due scale relative ad impatto e probabilità, si devono ora fornire le valutazioni relativa all'accesso illegittimo ai dati personali, alle modifiche indesiderate degli stessi e alla loro perdita.

3.1.4 VALUTAZIONI (INIZIALI) DI IMPATTO E DI PROBABILITÀ COMPLESSIVE

Sulla base delle informazioni riportate nei tre precedenti riquadri, si assegnano quindi una **valutazione dell'impatto** ed una **valutazione della probabilità** in corrispondenza di ognuna delle tre voci **ACCESSO ILLEGITTIMO DI DATI, MODIFICHE INDESIDERATE DEI DATI e PERDITA DI DATI** (ovvero: perdita di riservatezza, di integrità e di disponibilità) nella sottostante tabella.
Tra le valutazioni riferite a impatto e probabilità, si considerano quelle **più alte** come **valutazione complessiva dell'impatto** e **valutazione complessiva della probabilità.**

AMBITI DI RISCHIO	STIMA IMPATTO	STIMA PROBABILITÀ
- A - **PERDITA DI RISERVATEZZA: ACCESSO ILLEGITTIMO AI DATI PERSONALI**	*2*	*3*
- B - **PERDITA DI INTEGRITÀ:**	*4*	*3*

MODIFICA NON AUTORIZZATA DEI DATI PERSONALI		
- C - **PERDITA DI DISPONIBILITÀ: PERDITA, FURTO, CANCELLAZIONE NON AUTORIZZATA DEI DATI PERSONALI**	*4*	*3*
VALUTAZIONI COMPLESSIVE	*4*	*3<20%)*
	Nota: *per il totale valutazione, inserire la più alta tra le valutazioni riferite alle tre voci A, B e C*	***Nota:*** *per il totale valutazione, inserire la più alta tra le valutazioni riferite alle tre voci A, B e C*

3.1.5 VALUTAZIONE DEL RISCHIO INIZIALE

La valutazione del rischio è data ora dal prodotto del valore attribuito all'impatto per quello attribuito alla probabilità. Il valore minimo sarà quindi pari a 1, mentre quello più alto, corrispondente al massimo livello di rischio, sarà pari a 20.

I M P A T T O	**5 - Grave**				
	4 - Significativo			**12**	
	3 - Importante				
	2 - Limitato				
	1 - Trascurabile				
		1 - Trascurabile	**2 - Limitata**	**3 - Significativa**	**4 - Massima**
		P R O B A B I L I T À			

VALORE RISCHIO INIZIALE = IMPATTO X PROBABILITÀ = …

LIVELLO DI RISCHIO INIZIALE

LIVELLO DI RISCHIO INIZIALE minore di 7
rischio **BASSO** (colore VERDE)

LIVELLO DI RISCHIO INIZIALE compreso tra 7 e 11
rischio **MEDIO** (colore GIALLO)

LIVELLO DI RISCHIO INIZIALE RESIDUO maggiore di 11
rischio **ELEVATO** (colore ROSSO)

LIVELLO RISCHIO INIZIALE = IMPATTO x PROBABILITÀ = __12____ il rischio è _____Elevato_____

3.2 MISURE

Indicare quali siano le misure esistenti/pianificate per garantire la sicurezza dei dati.
Di seguito è riportato un elenco, indicativo e non esaustivo, delle misure che possono essere adottate per ridurre i rischi. E' necessario valutare di volta in volta quali misure sono utilizzabili, in relazione al trattamento, a riduzione dei singoli rischi.
Selezionare le opzioni SI, NO, NON SO inserendo una X tra le parentesi.

MISURE ORGANIZZATIVE / TECNICHE				
MISURE	**MISURA ADOTTATA ?**			**SVILUPPO/MIGLIORAMENTO**
Procedura gestione *data breach* *(specificare se vi sono procedure per limitare il rischio violazione dei dati)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Procedura di* applicazione delle misure tecniche ed organizzative adeguate a proteggere i dati personali e stabilire immediatamente se si è verificata una violazione; in caso affermativo tempestiva notifica all'Autorità di controllo ed eventuale comunicazione agli interessati
Nomina incaricati in forma scritta *(indicare se il personale autorizzato ad accedere e trattare i dati sia incaricato con atto scritto)*	**SI (X)**	**NO ( )**	**NON SO ( )**	
Istruzioni chiare e precise per gli incaricati *(indicare se il personale autorizzato ad accedere e trattare i dati riceva chiare istruzioni per iscritto)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Istruzione impartite all'atto di nomina dell'incaricato, in particolare sulle operazioni consentite in relazione al profilo di autorizzazione , vietando qualsiasi registrazione di immagini che appaiono sul monitor mediante qualsiasi dispositivo ivi inclusi telefoni cellulari.*
Formazione degli incaricati *(attività e programmi di formazione del personale incaricato del trattamento dei dati)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Il fornitore del sistema, oltre alla formazione del proprio personale dipendente, provvederà anche alla formazione del personale aziendale incaricato che gestirà il sistema stesso*
Conservazione di idonea documentazione comprovante formazione/istruzione personale incaricato *(specificare le modalità di conservazione di documentazione relativa alle attività di formazione e istruzione degli incaricati)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Archivio di Struttura*
Altre misure relative al personale autorizzato al trattamento *(specificare se sono previste altre misure relative alla gestione del personale autorizzato)*	**SI (x)**	**NO ( )**	**NON SO ( )**	*Attribuzione all'incaricato di credenziali personali di accesso al sistema;*
Procedura per la revisione periodica delle misure di sicurezza del trattamento *(specificare se vi sono procedure per la revisione periodica delle misure di sicurezza)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Aggiornamento periodico delle password, piano emergenza del PO, valutazione rischi;*
Procedure per limitare rischi di accesso da parte di soggetti non autorizzati ai documenti cartacei contenenti dati *(specificare se vi sono procedure per limitare il rischio di accesso da parte di non autorizzati)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*Non ci sono dati cartacei*
Contratto con il responsabile del trattamento *(specificare se vi sono responsabili ex art. 28 RGPD e, in caso positivo riportare nello spazio note a lato i*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Ditta esterna che si occuperà delle manutenzioni e aggiornamenti hardware e software*

trattamenti effettuati dal Responsabile)				
Controllo degli accessi fisici *(misure atte a impedire l'accesso fisico ai locali da parte di persone non autorizzate)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Limitazione dell'accesso ai locali dell'unità di memoria ai soli autorizzati;*
Crittografia *(misure atte a garantire che solo il mittente e il/i destinatari(o) di un messaggio ne conosca(no) il contenuto)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*In quanto trattasi di sistema a circuito chiuso*
Anonimizzazione *(misure atte ad eliminare definitivamente i rischi di re identificazione)*	**SI ( )**	**NO (x)**	**NON SO ( )**	*Non applicabile al trattamento in questione. Si ricorda che le riprese che puntano su postazioni fisse dei dipendenti sono settate in modo tale che le immagini relative agli stessi sono solarizzate. Inoltre le riprese sono effettuate con una scarsa definizione delle immagini, ciò consente di mettere a disposizione ai soli terzi legittimati le rappresentazioni ad alta definizione, le quali sono le uniche che consentono il riconoscimento,*
Pseudonimizzazione *(misure adottate affinché i dati personali non possano più essere attribuiti ad uno specifico interessato senza l'utilizzo di informazioni aggiuntive, che devono essere conservate separatamente)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Non applicabile al trattamento in questione.*
Archiviazione *(modalità di conservazione e gestione di archivi elettronici)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Archiviazione limitata a 72 ore con cancellazione automatica per sovrascrittura*
Sicurezza dei documenti cartacei *(modalità di gestione dei supporti cartacei utilizzati nel trattamento, come stampa, archiviazione, distruzione)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*Non ci sono dati cartacei*
Partizionamento e riduzione dell'accumulazione di dati *(misure atte a ridurre la possibilità di correlazioni fra i dati personali, ad esempio: distribuzione dei dati in sottosistemi indipendenti, etc.)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*Non ci sono dati cartacei*
Minimizzazione *(misure volte a garantire adeguatezza, pertinenza e limitazione dei dati oggetto di trattamento)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*Si rimanda al punto* 2.1.3;
Controllo degli accessi ai sistemi di trattamento dei dati (autenticazione) *(procedure di gestione degli accessi logici degli utenti a sistemi che trattano i dati, v. autenticazione)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Accesso attraverso password individuali consentito ad un numero limitato di soggetti*
Controllo degli accessi ai dati (profilazione) *(procedure di abilitazione differenziata nei sistemi di accesso, come profilazione, revisione periodica abilitazioni, etc.)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Gli operatori aziendali autorizzati ad accedere al sistema avranno un unico profilo*
Gestione delle postazioni di lavoro *(misure di sicurezza presenti e attive nelle postazioni di lavoro)*	**SI ( )**	**NO ( )**	**NON SO ( )**	*Non applicabile*

Tracciabilità *(misure per la registrazione degli accessi, es. file di log)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Saranno memorizzati gli accessi (utente, data, ora, ecc. per periodo di conservazione di **60 giorni** dall'evento. La cancellazione avviene automaticamente*
Gestione dell'emergenza – disponibilità e accesso ai dati in caso di incidente fisico o tecnico (*disaster recovery)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Piano di gestione emergenze*
Procedure di salvataggio *(periodicità backup)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*Cancellazione dati dopo 72 ore salvo richieste delle Autorità di Polizia o degli interessati;*
Manutenzione dei sistemi *(procedure di manutenzione fisica dei dispositivi, anche da parte del fornitore esterno)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Registri di Manutenzione tenuti dal Dipartimento Tecnico*
Sicurezza dell'hardware *(misure volte a garantire la sicurezza del materiale hardware)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Dettagli tecnici impianto come da documentazione, posizionamento videocamere in modo da contenere atti vandalici, collocazione unità di memoria in luogo protetto ad accesso controllato.*
Sicurezza del software *misure volte a garantire la sicurezza del software)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Dettagli tecnici software come da documentazione tecnica che sarà fornita dall'installatore*
Dispositivi mobili *(misure per utilizzo di smartphone, tablet, portatili, chiavette, etc.)*	**SI ( )**	**NO (x)**	**NON SO ( )**	*Gli autorizzati potranno fornire i dati ai terzi legittimati su dispositivi di proprietà di questi ultimi. L'azienda non fornisce alcun dispositivo di supporto.*
Sicurezza dei servizi di rete *(misure volte a garantire la sicurezza dei servizi di rete)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*I dati informatici non sono in rete*
Lotta contro il malware *(malware che potrebbe compromettere la sicurezza dei dati personali)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*I dati informatici non sono in rete*
Controllo della trasmissione dei dati *(procedure di controllo in caso di comunicazione elettronica o trasporto fisico dei dati)*	**SI ( )**	**NO (X)**	**NON SO ( )**	*I dati informatici non sono in rete*
Procedura e sistemi di emergenza *(esistenza di misure per evitare che fonti di rischio, umane o non umane, anche se scarsamente probabili, arrechino pregiudizio ai dati personali, es. pericolo di incendio, etc.)*	**SI (X)**	**NO ( )**	**NON SO ( )**	*Piano gestione emergenze*
Altre misure *(specificare)*	**SI ( )**	**NO (X)**	**NON SO ( )**	
Note: *Inserire eventuali note/osservazioni ulteriori*				

3.3 RISCHIO RESIDUO STIMATO

3.3.1 RIVALUTAZIONI DI IMPATTO E DI PROBABILITÀ COMPLESSIVE

Ora, alla luce delle misure di sicurezza e dei controlli sopra indicati, l'**impatto potenziale** e la **probabilità di accadimento** di un evento/minaccia sono rivalutati come segue.

Sulla base delle informazioni riportate nei tre precedenti riquadri, si assegnano – nella sottostante tabella - una **valutazione dell'impatto** ed una **valutazione della probabilità** in corrispondenza di ognuna delle tre voci **ACCESSO ILLEGITTIMO DI DATI, MODIFICHE INDESIDERATE DEI DATI e PERDITA DI DATI** (ovvero: perdita di riservatezza, di integrità e di disponibilità).

Ai fini del calcolo del rischio residuo stimato, le valutazioni **più alte** indicate nelle colonne *nuova stima impatto*

e *nuova stima probabilità* andranno a rappresentare la **valutazione complessiva dell'impatto** e la **valutazione complessiva della probabilità.**
L'indicazione dei nuovi valori è accompagnata dalle relative motivazioni.

AMBITI DI RISCHIO	**NUOVA STIMA IMPATTO**	**NUOVA STIMA PROBABILITÀ**
- A - **PERDITA DI RISERVATEZZA: ACCESSO ILLEGITTIMO AI DATI PERSONALI**	**- 2 -**	**- 1 -**
	Motivazione: *L'impatto di un eventuale accesso illegittimo resta comunque il medesimo*	**Motivazione:** *L' accesso autorizzato e limitato al preposto o agli autorizzati mediante Chiavi di accesso e riduce fortemente la probabilità di errori connessi al fattore umano.*
- B - **PERDITA DI INTEGRITÀ: MODIFICA NON AUTORIZZATA DEI DATI PERSONALI**	**Motivazione:** *4*	*1*
	Motivazione: *L'impatto di una modifica non autorizzata del dato resta comunque grave*	**Motivazione:** *L'accesso autorizzato e limitato al preposto o a pochi delegati mediante chiavi di accesso riduce fortemente la Probabilità di errori connessi al fattore umano .inserire valore)*
- C - **PERDITA DI DISPONIBILITÀ: PERDITA, FURTO, CANCELLAZIONE NON AUTORIZZATA DEI DATI PERSONALI**	***4***	***1***
	Motivazione: *L'impatto su una eventuale accesso illegittimo resta comunque grave*	**Motivazione:** *scrivere motivazione* *Es. Le misure tecniche adottate consentono di ridurre il rischio di perdita dei dati / indisponibilità temporanea dei dati (specificare…)*
RIVALUTAZIONI COMPLESSIVE	***4***	**1**
	***Nota:** per il totale valutazione, inserire la più alta tra le valutazioni riferite alle tre voci A, B e C*	***Nota:** per il totale valutazione, inserire la più alta tra le valutazioni riferite alle tre voci A, B e C*

3.3.2 VALUTAZIONE DEL RISCHIO RESIDUO

La valutazione del rischio è data dal prodotto del valore attribuito all'impatto per quello attribuito alla probabilità. Il valore minimo sarà quindi pari a 1, mentre quello più alto, corrispondente al massimo livello di rischio, sarà pari a 20.

IMPATTO		5 - Grave				
		4 - Significativo	4			
		3 - Importante				
		2 - Limitato				
		1 - Trascurabile				
			1 - Trascurabile	2 – Limitata	3 - Significativa	4 - Massima
			PROBABILITÀ			

VALORE RISCHIO RESIDUO = IMPATTO X PROBABILITÀ = 4

LIVELLO DI RISCHIO RESIDUO

LIVELLO DI RISCHIO RESIDUO minore di 7
rischio **BASSO e ACCETTABILE** (colore VERDE): non è necessario prevedere azioni di adeguamento ma è possibile valutare delle azioni per il miglioramento/ottimizzazione del sistema di prevenzione e protezione dal rischio

LIVELLO DI RISCHIO RESIDUO compreso tra 7 e 11
rischio **MEDIO** (colore GIALLO): è consigliato individuare azioni di adeguamento delle misure applicate oppure introdurre nuove misure più efficaci a protezione del trattamento analizzato

LIVELLO DI RISCHIO RESIDUO maggiore di 11
rischio **ELEVATO** (colore ROSSO): non si è in grado di trovare misure adeguate a ridurre il rischio residuo a livello medio/basso; il trattamento non può essere iniziato ed è obbligatorio richiedere la consultazione preventiva dell'Autorità Garante in relazione al trattamento oggetto della DPIA. Tale adempimento deve essere considerato parte integrante dello stesso processo di DPIA. Ai fini dell'attivazione della consultazione il Preposto si raccorda con il Responsabile Protezione Dati.

LIVELLO RISCHIO RESIDUO = IMPATTO x PROBABILITÀ = __4___ il rischio è _Basso__BASSO E ACCETTABILE__

*4.*PIANO DI TRATTAMENTO RISCHIO RESIDUO

Descrivere il piano d'azione con le misure/azioni correttive previste per migliorare la sicurezza del trattamento in caso di livello di rischio residuo MEDIO *o* BASSO

Per il trattamento del Rischio Residuo non é possibile agire né sull'impatto, nè sulla frequenza; il primo risulta dipendente da medesime potenziali conseguenze in tutte le analisi effettuate , per i possibili errori interpretativi di immagini da parte degli organi deputati , la seconda dipendente dalla imprevedibilità di accadimenti atmosferici estremi e dal rischio connesso ad eventi imponderabili come terremoti , incendi ,allagamenti ecc, o furti che possono alterare le immagini o mettere fuori uso l'impianto .

Infatti tutte le misure di abbattimento del rischio residuo risultano già in atto.

Esempi sono la Certificazione Antincendio, la installazione sotto gruppo di Continuità, Accessi ai locali dei soli autorizzati oltre che alle Ditte di manutenzione dei prodotti

Parere degli interessanti ( ) È stato chiesto il parere degli interessati (X) Non è stato chiesto il parere degli interessati	Motivazione: Trattasi di pluralità indeterminata di soggetti (pazienti , accompagnatori, dipendenti di fornitori, operatori vari cui è impossibile raccogliere eventuale parere) Relativamente al personale dipendente dell'Azienda le telecamere che saranno installate potranno incidentalmente riprendere i lavoratori dell'Azienda Usl Toscana sud est e per questo motivo ai sensi dell'art.4 della Legge n.300/1970 e s.m.i. Statuto dei Lavoratori si procederà alla sottoscrizione di specifico accordo con le Organizzazioni Sindacali.

Contrassegnare con "X" tra le parentesi l'opzione che si intende indicare, motivando a lato la scelta.

Data e Luogo

firma

LUCIA GRAZIA
CAMPANILE
Regione
Toscana/01386030488
10.04.2025 10:51:55
GMT+01:00