Azienda Provinciale per i Servizi Sanitari
Provincia Autonoma di Trento

Estratto della Valutazione di Impatto

(*Data Protection Impact Assessment* - DPIA)
sulla protezione dei dati personali

relativa al progetto di ricerca

EFRAIM 3: Studio multicentrico per migliorare la gestione e l'esito clinico di pazienti immunocompromessi con insufficienza respiratoria acuta

redatta ai sensi dell'art. 35 del Reg. UE 679/2016 (GDPR)

e sulla base delle Linee Guida del 4/10/2017 del Working Party Art. 29

TITOLARE DEL TRATTAMENTO / CONTITOLARI	AZIENDA PROVINCIALE PER I SERVIZI SANITARI DELLA PROVINCIA AUTONOMA DI TRENTO
TITOLO DELLO STUDIO	STUDIO MULTICENTRICO PER MIGLIORARE LA GESTIONE E L'ESITO CLINICO DI PAZIENTI IMMUNOCOMPROMESSI CON INSUFFICIENZA RESPIRATORIA ACUTA
CODICE DELLO STUDIO	EFRAIM 3
REDATTORI	DOTT. ALBERTO CUCINO (PRINCIPAL INVESTIGATOR), UNITA' OPERATIVA DI ANESTESIA E RIANIMAZIONE 1, OSPEDALE SANTA CHIARA, AZIENDA PROVINCIALE PER I SERVIZI SANITARI DELLA PROVINCIA AUTONOMA DI TRENTO, PROVINCIA DI TRENTO
VERIFICATORE INTERNO	DOTT. EMANUELE TORRI
DPO	AVV. SILVIA STEFANELLI
VERSIONE	1
DATA REVISIONE	27/08/2024

1. Definizione del contesto.

In questa sezione è analizzata nel dettaglio e sotto diversi punti di vista l'attività di trattamento da sottoporre a valutazione.

1.1 La titolarità del trattamento.

In questo paragrafo sono individuati i soggetti in capo ai quali sussiste la titolarità del trattamento dei dati personali oggetto della presente valutazione di impatto.

1.1.1 Titolare.

Il Titolare è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

	In caso di titolarità autonoma (un solo Titolare) inserire i dati del Titolare del trattamento.

RAGIONE SOCIALE	AZIENDA PROVINCIALE PER I SERVIZI SANITARI DELLA PROVINCIA AUTONOMA DI TRENTO(APSS)
SEDE LEGALE	VIA DEGASPERI 79, 38123 TRENTO
INDIRIZZO MAIL	dirgen@apss.tn.it
INDIRIZZO PEC	apss@pec.apss.tn.it
DPO	responsabileprotezionedati@apss.tn.it

1.2 Individuazione generale dell'attività di trattamento *(a cura del P.I. e dei Ricercatori).* In questo paragrafo sono individuate le caratteristiche generali dello studio clinico.

1.2.a Breve descrizione del progetto di ricerca 	Un terzo dei pazienti critici sono immunocompromessi e l'insufficienza respiratoria acuta (ARF) è per loro la prima causa di ingresso in terapia intensiva. Negli ultimi anni la sopravvivenza di questi pazienti è migliorata. Per ottenere i migliori risultati possibili, è stato stabilito uno standard of care basato sul ricovero precoce in terapia intensiva e sulla gestione non invasiva dell'ARF, e sono dunque state definite le priorità della ricerca. Questo studio, che include 10.000 pazienti immunocompromessi con ARF distribuiti in 21 Paesi, si pone l'obiettivo di valutare la mortalità a 90 giorni dopo l'ammissione in terapia intensiva, con particolare attenzione all'outcome dei pazienti con indeterminata eziologia dell'ARF. Verranno anche individuati i determinanti che portano alla necessità di incrementare il supporto respiratorio standard a quello massimale, includendo l'intubazione o altre strategie di salvataggio in uso. La durata dello studio è di 6 anni.	È possibile allegare il documento che riporta la sinossi o un diagramma di flusso che descrive l'attività di trattamento dei dati nell'ambito dello studio (All. n. 1)
1.2.b Tipo di ricerca 	☐ Studio unicentrico X Sudio multicentrico X Studio osservazionale ☐ Studio sperimentale con farmaco ☐ Indagine clinica con dispositivo medico ☐ Studio interventistico senza dispositivi e senza farmaci ☐ Studio esclusivamente su materiali biologici ☐ Altro	
1.2.c Dati raccolti 	Nell'ambito della ricerca vengono raccolte informazioni riguardanti: X L'identità dei partecipanti X Lo stato di salute dei partecipanti ☐ Dati genetici SPECIFICARE: - Variabili demografiche e quelle caratterizzano le comorbidità del paziente (diabete, ipertensione, insufficienza cardiaca, respiratoria o renale, malattie neurologiche progressive, ecc.), nonché le condizioni generali del paziente, utilizzando il Performance status. - Variabili che descrivono la patologia tumorale: tipo di cancro o di malignità ematologica, stadio alla diagnosi, tempo intercorso tra la diagnosi e il ricovero in terapia intensiva, trattamenti intrapresi, risposta ai trattamenti. - Caratteristiche dell'insufficienza respiratoria: severità, gestione della dipendenza da ossigeno, eziologia, esami effettuati (prima e durante la degenza in terapia intensiva), trattamenti effettuati. - Stato del paziente alla dimissione dalla terapia intensiva, dall'ospedale e a 3 mesi X Altro SPECIFICARE:	

	- Caratteristiche della terapia intensiva: descrizione della malattia acuta, misurazioni giornaliere di insufficienza d'organo, diagnosi definitiva (sepsi, tossicità dei trattamenti, infiltrazioni maligne maligna o altro), durata dei principali trattamenti intrapresi (ossigenazione umidificata ad alto flusso, ventilazione non invasiva, ventilazione meccanica invasiva, catecolamine, dialisi, trasfusioni, chemioterapia), eventuali decisioni di limitare l'attività del paziente, terapia attiva (non aumento della terapia, interruzione del supporto d'organo). Infezioni fungine, da batteri multi resistenti ai farmaci e la comparsa di infezioni nosocomiali. - Caratteristiche del centro dove viene svolto lo studio
1.2.d Consenso informato 	Viene prevista l'acquisizione del consenso informato **allo studio**: X **SI** (se possibile) ☐ **NO**
1.2.e Comitato Etico 	Il progetto di ricerca ha ottenuto **motivato parere favorevole** dal competente Comitato Etico a livello territoriale? X **SI** ☐ **NO** ☐ in corso di sottomissione

4. Tabelle di calcolo del rischio e valutazione dell'impatto sugli interessati.

In questa sezione del documento è dettagliata l'analisi del rischio del trattamento oggetto della valutazione d'impatto.

La definizione di rischio è la seguente:

> *il rischio è l'eventualità di subire un danno in conseguenza di un'azione compiuta o subita, e si calcola ricorrendo alla formula **R=P*I**, in cui **P** è la probabilità di accadimento delle minacce, e **I** è l'impatto o danno conseguente.*[1]

Alla luce della definizione di cui sopra, l'analisi del rischio viene svolta nel seguente modo:

- prima vengono analizzate le **minacce** e la **probabilità di accadimento delle minacce**;
- poi viene analizzato **l'impatto** o danno conseguente in caso di accadimento;
- tenuto conto poi delle minacce e del possibile impatto, viene valutato il **rischio**.

Tale rischio è denominato **rischio inerente:** vale a dire il rischio connaturato nell'attività svolta dall'organizzazione prima dell'adozione di misure volte a contenerlo o controllarlo.

In sostanza, si opera una valutazione dei rischi intrinseci cui è esposta l'organizzazione senza che si operi un controllo sugli stessi[2].

Valutato il rischio inerente si andranno ad analizzare le misure di sicurezza implementate o che si reputa opportuno implementare per valutare il rischio residuo.

Il **rischio residuo** è il rischio che permane dopo aver implementato le misure di sicurezza sul rischio inerente[3].

Infine:

- Se il rischio residuo viene valutato come **accettabile**, potrà procedersi con l'attività di trattamento dei dati.
- Se il rischio residuo viene invece valutato come **non accettabile** (in quanto continui ad essere elevato nonostante le misure di sicurezza adottate), sarà necessario svolgere la Consultazione preventiva dinanzi l'Autorità Garante ai sensi dell'art. 36 GDPR.

NB: La compilazione delle tabelle riportate ai successivi paragrafi 4.1., 4.2. e 4.3. deve seguire le istruzioni riportate nell'Allegato 1.

1 Guida ISO/IEC 73/2009, 3.6.1.8: il rischio può esser definito come la combinazione delle probabilità di un evento e delle sue conseguenze;
2 Guida ISO/IEC 73/2009, 3.6.1.8: L'identificazione del rischio comporta l'individuazione delle fonti di rischio (3.5.1.2), degli eventi (3.5.1.3), delle loro cause e delle loro potenziali conseguenze (3.6.1.3). L'identificazione del rischio può coinvolgere dati storici, analisi teoriche, opinioni informate ed esperte e le esigenze delle parti interessate.
3 Guida ISO/IEC 73/2009: 3.8.1.6 rischio residuo: rischio (1.1) rimanente dopo il trattamento del rischio (3.8.1)

4.1. Perdita di riservatezza *(a cura del P.I., Ricercatori, del Personale Tecnico e del Referente Privacy limitatamente al punto 3 della tabella sottostante).*

☐ **La perdita di riservatezza dei dati non ha impatto sui diritti e le libertà degli interessati**	**Se è stata spuntata questa casella, la tabella sotto riportata NON deve essere compilata**

Divulgazione/ accesso non autorizzato o accidentale	

1. Quali sono le **potenziali minacce** alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	☐ Accesso abusivo da parte di persone non autorizzate ai luoghi in cui si svolge il trattamento (es. sala CED, archivio dei documenti, uffici con computer, laboratori ecc.) ☐ Sottrazione da parte di soggetti interni o esterni alla struttura di documenti cartacei o di strumenti elettronici (pc) X Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransmoware, etc.) ☐ Intercettazione del traffico Ethernet; acquisizione dei dati inviati su una rete Wi-Fi, ☐ Condivisione dei dati con soggetti non autorizzati ☐ _____	
2. Quali sono le principali **vulnerabilità** rilevate?	☐ Salvataggio dei dati su chiavette USB o dischi esterni personali ☐ Inefficacia delle tecniche di pseudonimizzazione o crittografia X Mancata formazione del personale o formazione risalente ☐ Locali non protetti da accessi esterni ☐ Strumenti non protetti da attacchi informatici ☐ Mancata adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ _____	
3.**Conseguenze per gli interessati della perdita di riservatezza dei dati:**	Impatto sui **diritti e le libertà** degli interessati:	**Livello di impatto** della perdita di riservatezza dei dati:
☐ Morte	Diritto alla vita (art. 2 Cost.)	X Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
☐ Perdite finanziarie	Diritti patrimoniali	
X Perdita di riservatezza dei dati personali protetti da segreto professionale	Rivelazione del segreto professionale (art. 622 c.p.)	
X Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	
4. Stima della **probabilità** di accadimento delle minacce	X Improbabile 1 ☐ Poco probabile 2	

(fattore **P** della formula di calcolo del Rischio)	☐ Probabile 3 ☐ Molto probabile 4
5. Stima dell'**impatto** (fattore **I** della formula di calcolo del Rischio)	X Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4

6. **Rischio inerente** (R = P x I)

		P			
		Improbabile	Poco probabile	Probabile	Molto probabile
I	Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
	Grave	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali **misure di sicurezza** già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	☐ crittografia [*descrizione delle tecniche di crittografia*:_____] X pseudonimizzazione [*descrizione delle tecniche di pseudonimizzazione*:_____] X limitazione degli accessi [*descrizione delle modalità*:_____] X Misure di protezione dagli attacchi informatici [*descrizione delle misure*:_____] ☐ Adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ Formazione del personale ☐ _____			
8. Misure di sicurezza:	X adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. **Stima del rischio residuo**

		Misure di sicurezza			
		Adeguate	Minime	Insufficienti	Inesistenti
R_i	Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
	Alto	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Basso	☐ 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. **Modalità di mitigazione del rischio** per gestire il rischio residuo	X nessuna: accettazione del rischio (1-6) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____
11. Quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	• _____
12. Priorità degli **interventi** di attuazione delle ulteriori misure di sicurezza	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5)

	☐ entro 1 mese (6-8) ☐ immediata (9-16)
13. **Responsabile/i** dell'attuazione delle ulteriori misure di sicurezza	1. 2.

14. **Rischio residuo**	X accettabile (1-6)	☐ non accettabile (8-16)
	attuazione del trattamento	consultazione preventiva

4.2. Perdita di integrità *(a cura del P.I., Ricercatori, del Personale Tecnico e del Referente Privacy limitatamente al punto 3 della tabella sottostante).*

☐ La perdita di integrità dei dati non ha impatto sui diritti e le libertà degli interessati	**Se è stata spuntata questa casella, la tabella sotto riportata NON deve essere compilata**

Modifica non autorizzata o accidentale	
1. Quali sono le **potenziali minacce** alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	☐ Malfunzionamento dell'hardware ☐ Malfunzionamento del software ☐ Deterioramento degli strumenti informatici X Errore umano nell'inserimento dei dati ☐ Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransmoware, etc.)
2. Quali sono le principali **vulnerabilità** rilevate?	☐ Mancanza di regolarità nella manutenzione dell'hardware ☐ Mancanza di regolarità nell'aggiornamento del software ☐ Strumenti non protetti da attacchi informatici ☐ Mancata adozione di una policy per il corretto utilizzo degli strumenti informatici X Mancata formazione del personale ☐ _____

3.**Conseguenze per gli interessati della perdita di integrità dei dati:**	Impatto sui **diritti e le libertà** degli interessati:	**Livello di impatto** della perdita di integrità dei dati:
☐ Morte	Diritto alla vita (art. 2 Cost.)	X Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
☐ Perdite finanziarie	Diritti patrimoniali	
X Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	
4. Stima della **probabilità** di accadimento delle minacce	X Improbabile 1 ☐ Poco probabile 2	

(fattore **P** della formula di calcolo del Rischio)	☐ Probabile 3 ☐ Molto probabile 4
5. Stima dell'**impatto** (fattore **I** della formula di calcolo del Rischio)	X Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4

6. **Rischio inerente** (R = P x I)

		P			
		Improbabile	Poco probabile	Probabile	Molto probabile
I	Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
	Grave	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali **misure di sicurezza** già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	X Regolare manutenzione dell'hardware X Software aggiornato regolarmente X Adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ Formazione del personale X Doppio controllo nell'inserire i dati nella eCRF			
8. Misure di sicurezza:	X adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. **Stima del rischio residuo**

		Misure di sicurezza			
		Adeguate	Minime	Insufficienti	Inesistenti
R_i	Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
	Alto	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Basso	☐ 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. **Modalità di mitigazione del rischio** per gestire il rischio residuo	X nessuna: accettazione del rischio (1-6) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____
11. Quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	• _____
12. Priorità degli **interventi** di attuazione delle ulteriori misure di sicurezza	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
13. **Responsabile/i** dell'attuazione delle ulteriori misure di sicurezza	1. 2.

14. **Rischio residuo**	X accettabile (1-6)	☐ non accettabile (8-16)
	attuazione del trattamento	consultazione preventiva

4.3. Perdita di disponibilità *(a cura del P.I., Ricercatori, del Personale Tecnico e del Referente Privacy limitatamente al punto 3 della tabella sottostante).*

X La perdita di disponibilità dei dati non ha impatto sui diritti e le libertà degli interessati	**Se è stata spuntata questa casella, la tabella sotto riportata NON deve essere compilata**

Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale	
1. Quali sono le **potenziali minacce** alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	☐ Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransmoware, etc.) ☐ Catastrofi naturali (incendi, allagamenti, terremoti) ☐ Eliminazione accidentale dei dati ☐ _____
2. Quali sono le principali **vulnerabilità** rilevate?	☐ Assenza di impianto antincendio ☐ Conservazione dei dati in locali seminterrati o vicino a tubature ☐ Zona sismica ☐ Strumenti non protetti da attacchi informatici ☐ Mancata formazione del personale ☐ _____

3.**Conseguenze per gli interessati della perdita di disponibilità dei dati:**	Impatto sui **diritti e le libertà** degli interessati:	**Livello di impatto** della perdita di disponibilità dei dati:
☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4 ☐ La perdita di disponibilità non è configurabile
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
☐ Perdite finanziarie	Diritti patrimoniali	
☐ Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	

4. Stima della **probabilità** di accadimento delle minacce (fattore **P** della formula di calcolo del Rischio)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
5. Stima dell'**impatto** (fattore **I** della formula di calcolo del Rischio)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3

	☐ Gravissimo 4

6. **Rischio inerente** (R = P x I)

		P			
		Improbabile	Poco probabile	Probabile	Molto probabile
I	Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
	Grave	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali **misure di sicurezza** già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	☐ Misure di protezione dagli attacchi informatici [*descrizione delle misure*:_____] ☐ Backup [*descrizione delle modalità di backup*:_____] ☐ Cloud [*descrizione del cloud*:_____] ☐ Formazione del personale ☐ _____

8. Misure di sicurezza:	☐ adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. **Stima del rischio residuo**

		Misure di sicurezza			
		Adeguate	Minime	Insufficienti	Inesistenti
R_i	Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
	Alto	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Basso	☐ 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. **Modalità di mitigazione del rischio** per gestire il rischio residuo	☐ nessuna: accettazione del rischio (1-6) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____
11. Quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	• _____
12. Priorità degli **interventi** di attuazione delle ulteriori misure di sicurezza	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
13. **Responsabile/i** dell'attuazione delle ulteriori misure di sicurezza	1. 2.

14. **Rischio residuo**	☐ accettabile (1-6)	☐ non accettabile (8-16)
	attuazione del trattamento	consultazione preventiva

5.CONCLUSIONI *(a cura del Referente Privacy in base anche a quanto rilevato dal DPO).*

5.1 Valutazione finale.

Il Titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché delle diverse probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento. Dette misure saranno riesaminate e aggiornate qualora necessario.
Nelle precedenti sezioni di questa DPIA:

- è stato presentato definito il contesto e presentato il processo di trattamento dei dati personali;
- sono state descritte le caratteristiche del trattamento dei dati;
- sono state individuate e analizzati – in rapporto alle differenti minacce – i rischi per l'interessato conseguenti alla perdita di riservatezza, integrità e disponibilità dei dati e le misure di sicurezza in atto per la mitigazione di tali rischi;
- sono state identificate le vulnerabilità nell'adozione delle misure di sicurezza in atto e indicate contromisure alla mitigazione del rischio.

Nella Sezione successiva si andrà a riportare se permane un rischio residuo elevato e se risulti pertanto necessaria una consultazione preventiva con l'Autorità Garante per la protezione dei dati personali.

5.2 Rischio residuo.

Ai sensi del GDPR, se il rischio residuo a fronte dell'adozione delle contromisure rimane elevato, deve essere consultata l'Autorità Garante per la protezione dei dati personali.
Il Gruppo di Lavoro Articolo 29 (WP29) nelle Linee Guida sulla DPIA definisce come rischio residuo elevato inaccettabile quello che caratterizza i "*casi in cui le persone gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad es. accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad es. poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilità ben nota*)".

Il Titolare ha concluso che, considerate le misure di sicurezza in atto e pianificate e le contromisure che verranno attuate nei tempi indicati dalla presente DPIA, nel trattamento di dati oggetto della presente DPIA, non si rilevano condizioni di rischio residuo elevato e che pertanto non è necessario consultare l'Autorità garante ai sensi dell'art. 36 del GDPR.

Il Titolare del trattamento

_____