Azienda Provinciale per i Servizi Sanitari
Provincia Autonoma di Trento

Valutazione di impatto sulla protezione dei dati personali

(Estratto)

relativa al progetto di ricerca

Rates and Causes of Hospitalization in patients with ANCA-associated vasculitis: a retrospective observational study (REACH-AAV)

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 (APSS)
Titolo dello studio	Rates and Causes of Hospitalization in patients with ANCA-associated vasculitis: a retrospective observational study (REACH-AAV)
Codice dello studio	REACH-AAV
Redattori	Dott. Alvise Berti (Principal Investigator)
Verificatore interno	Dott. Emanuele Torri
DPO	Avv. Silvia Stefanelli
Versione	1
Data Revisione	08/10/2024

1. Sommario

2. Obiettivo e organizzazione del documento.

Il presente documento, redatto ai sensi dell'art. 35 del Reg. UE 2016/679 ("GDPR") e sulla base delle Linee Guida del 4 ottobre 2017 del Working Party Art. 29, ha lo scopo di valutare l'impatto sui diritti e le libertà delle persone fisiche con riferimento al trattamento dei dati effettuato nell'ambito del progetto di ricerca analizzato.

Ai sensi dell'art. 35 del GDPR la valutazione di impatto (o "DPIA") deve essere effettuata quando un'attività di trattamento di dati personali è in grado di determinare un rischio elevato per i diritti e le libertà delle persone fisiche alle quali i dati si riferiscono (interessati).

La Valutazione di Impatto deve essere effettuata **prima** di mettere in atto il trattamento dei dati personali ([1]), coerentemente con il principio di privacy by design e privacy by default ([2]) per individuare la necessità di implementare misure di sicurezza ulteriori rispetto a quelle già in atto e finalizzate a mitigare i rischi.

Nel valutare l'impatto del trattamento effettuato dai titolari o responsabili, sono tenute in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'art. 40 del GDPR e le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, raccolte laddove possibile.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Nel rispetto dei principi di cui all'art. 35 GDPR e Linee guida applicabili, la presente valutazione d'impatto è elaborata seguendo gli step sotto riportati.

1. Definizione del contesto in cui avviene l'attività di trattamento
2. Descrizione sistematica dell'attività di trattamento, con particolare attenzione al flusso dei dati
3. Indicazione delle modalità di rispetto dei principi applicabili al trattamento dei dati personali ([3])
4. Indicazione delle modalità di gestione dei diritti degli interessati ([4])
5. Indicazione del rispetto degli adempimenti relativi ai responsabili del trattamento ([5]) e degli autorizzati al trattamento ([6])
6. Definizione dei meccanismi dell'eventuale trasferimento dei dati in Paesi

[1] Considerando 90 e 93, art. 35, parr. 2 e 10, GDPR.
[2] Considerando 78, art. 25 GDPR.
[3] Art. 5 GDPR.
[4] Artt. 15-22 GDPR.
[5] Art. 28 GDPR
[6] Art. 29 GDPR e art. 2-*quaterdecies* D. Lgs. 196/2003 (Codice Privacy).

extra UE ([7]);
7. Calcolo del rischio relativo al trattamento
8. Indicazione delle minacce a cui è esposta l'attività di trattamento, calcolo del rischio inerente (probabilità e impatto), indicazione delle misure in atto, calcolo del rischio residuo, individuazione delle eventuali contromisure di mitigazione, valutazione dell'accettabilità del rischio residuo per verificare se mettere in atto il trattamento o ricorrere allo strumento della consultazione preventiva al Garante per la protezione dei dati personali ([8]).

La metodologia seguita per la redazione della DPIA soddisfa gli standard richiesti dal GDPR in quanto conforme ai criteri previsti dall' "Allegato 2 – Criteri per una DPIA ammissibile" alle Linee guida sulla Valutazione d'Impatto nella protezione dei dati (DPIA) e stabilire se il trattamento "può comportare un rischio elevato" ai sensi del regolamento 2016/679 (WP 248 rev.01).

[7] Capo V GDPR.
[8] Art. 36 GDPR.

3. Definizione del contesto.

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

3.1 Elementi di fatto

L'Azienda Provinciale per i Servizi Sanitari della Provincia Autonoma di Trento (di seguito "APSS") è l'ente strumentale della Provincia Autonoma di Trento preposto alla gestione coordinata delle attività sanitarie e socio-sanitarie per l'intero territorio provinciale.

La presente DPIA valuta il trattamento dei dati personali nell'ambito del progetto di ricerca "Rates and Causes of Hospitalization in patients with ANCA-associated vasculitis: a retrospective observational study (REACH-AAV)" promosso da APSS. Lo sperimentatore principale di questo studio è il Dott. Alvise Berti.

In particolare, il progetto di ricerca consiste in uno studio osservazionale, retrospettivo e multicentrico nel quale verranno raccolti dati clinico-anamnestici e relativi alle ospedalizzazioni dei pazienti con vasculite ANCA-associata per valutare i tassi stardardizzati di ospedalizzazione di questi pazienti rispetto alla popolazione italiana generale.

3.2 Ruoli privacy

Sono di seguito riportati i riferimenti dei soggetti che rivestono dei ruoli privacy nell'ambito delle attività del trattamento.

a) Titolare del trattamento

TITOLARE DEL TRATTAMENTO	
RAGIONE SOCIALE	**Azienda Provinciale per i Servizi Sanitari della Provincia Autonoma di Trento**
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

b) Contitolari del trattamento

Non applicabile

c) Responsabili del trattamento

AUSL –IRCCS di Reggio Emilia, con sede in 42122 Reggio Emilia, Via Amendola, n. 2

3.3 Descrizione generale dell'attività di trattamento

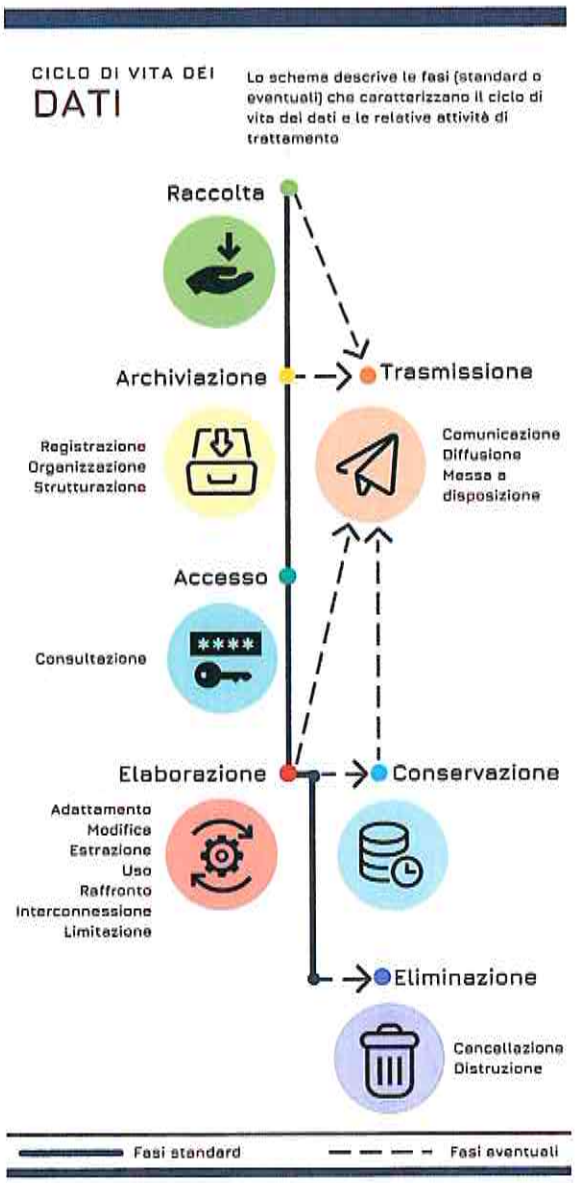
In questo paragrafo sono individuate le caratteristiche generali del progetto.

BREVE DESCRIZIONE DEL PROGETTO DI RICERCA	Lo studio è multicentrico e segue un disegno osservazionale retrospettivo. La raccolta retrospettiva dei dati clinico-anamnestici e relativi alle ospedalizzazioni dei pazienti con vasculite ANCA-associata (AAV) e con ricovero nel periodo dal 01/01/2007 al 31/12/2018 avverrà per mezzo della consultazione della cartella clinica elettronica ospedaliera. L'obiettivo primario di questo studio è di valutare retrospettivamente i tassi standardizzati di ospedalizzazione nei pazienti con AAV (per qualsiasi causa) rispetto alla popolazione italiana generale. Si prevede di raccogliere dati relativi a circa 500 pazienti, assumendo che 12 centri parteciperanno allo studio. Secondariamente saranno valutati: le cause del ricovero, la durata del ricovero ed intensità; i fattori di rischio per ospedalizzazione; i tassi standardizzati rispetto alla popolazione generale e la caratterizzazione della mortalità ospedaliera associata.
TIPO DI RICERCA	☐ Studio unicentrico X Studio 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
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: - Dati personali comuni: anno di nascita, sesso

	- Dati particolari relativi alla salute: valutazione clinica alla diagnosi di AAV, le date di esordio, di diagnosi, le date di ospedalizzazione, le tipologie e la durata dei trattamenti, eventuali riospedalizzazioni - Dati particolari relativi all'origine razziale o etnica ☐ Altro SPECIFICARE: _____
CONSENSO INFORMATO	Viene prevista l'acquisizione del consenso informato allo studio: X SI (per i soggetti ancora in vita) X NO (soggetti non raggiungibili o deceduti)
COMITATO ETICO	Il progetto di ricerca ha ottenuto motivato parere favorevole dal competente Comitato Etico a livello territoriale? X SI, parere di data 12/09/2024 ☐ NO ☐ in corso di sottomissione

4. Rappresentazione del ciclo di vita dei dati

Segue l'immagine che rappresenta il ciclo di vita dei dati, suddiviso in quattro fasi che comprendono le operazioni elencate nell'art. 4, 2 del GDPR.



6. 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.[9]

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[10].

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[11].
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.

---

9 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;

10 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.

11 Guida ISO/IEC 73/2009: 3.8.1.6 rischio residuo: rischio (1.1) rimanente dopo il trattamento del rischio (3.8.1)

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

6.1. Perdita di riservatezza

Perdita di riservatezza	La perdita di riservatezza dei dati ha impatto sui diritti e le libertà degli interessati? X SI > compilare il paragrafo 6.1 ☐ NO > passare al paragrafo 6.2

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?	X 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.) X 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 (fattore P della formula di calcolo del Rischio)	X Improbabile 1 ☐ Poco probabile 2 ☐ 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	X 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*: Sigla del centro – seguito da numero progressivo del paziente raccolto (es. TN-001)]
X limitazione degli accessi [*descrizione delle modalità*: accesso consentito solo con nome utente e password]
X Misure di protezione dagli attacchi informatici [*descrizione delle misure*: vedi misure adottate in APSS]
X 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	X 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

6.2. Perdita di integrità

Perdita di integrità	La perdita di integrità dei dati ha impatto sui diritti e le libertà degli interessati? X SI > compilare il paragrafo 6.2 ☐ NO > passare al paragrafo 6.3

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?	X Malfunzionamento dell'hardware X Malfunzionamento del software X Deterioramento degli strumenti informatici X Errore umano nell'inserimento dei dati

	X Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransomware, 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 (fattore P della formula di calcolo del Rischio)	X Improbabile 1 ☐ Poco probabile 2 ☐ 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	X 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 eCFR

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	X 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

6.3. Perdita di disponibilità

Perdita di disponibilità	La perdita di disponibilità dei dati ha impatto sui diritti e le libertà degli interessati? ☐ SI > compilare il paragrafo 6.3 X NO > passare al paragrafo successivo.

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, ransomware, 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
☐ 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)	configurabile
☐ 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

7. Conclusioni

7.1 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 definito il contesto e presentato il processo di trattamento dei dati personali;
- sono state descritte le caratteristiche del trattamento dei dati;
- sono stati individuati 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.

7.2 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
APSS – Il Direttore generale

8. Allegato 1 - Indicazioni per il calcolo del rischio

[Istruzioni per la compilazione delle Tabelle riportate al Paragrafo 6]
[NON COMPILARE questo allegato]

In questa sezione sono riportate le indicazioni per la compilazione delle tabelle di calcolo del rischio presenti nel paragrafo 8, ove sono presentati gli elementi – a livello macro – esposti alle minacce di:

Perdita della **RISERVATEZZA** dei dati	Perdita della **INTEGRITÀ** dei dati	Perdita della **DISPONIBILITÀ** dei dati

Per ogni elemento:

1. indicare le principali **minacce** suddivisibili in azioni esterne o interne *(si possono aggiungere quelle non previste)*

1. Quali sono le potenziali minacce alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	**Azioni intenzionali esterne o interne** ☐ **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, ecc.)**

2. indicare le principali **vulnerabilità** - intese come scarsa qualità dei mezzi impiegati che genera punti di debolezza

2. Quali sono le principali vulnerabilità rilevate?	**Indicare le vulnerabilità rilevate**

3. indicare le conseguenze per gli interessati e il livello di **impatto sui diritti e le libertà degli interessati** per ognuno dei tre requisiti di sicurezza (riservatezza, integrità, disponibilità) in base alla scala riportata di seguito. Si tratta di una scala di tipo "semi quantitativo", ovvero, la valutazione è guidata dal criterio (espresso in termini qualitativi) che corrisponde al livello (espresso in termini qualitativi) e al valore (espresso in termini numerici). ([12])

CRITERIO	LIVELLO	VALORE
Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).	Lieve	1

[12] La natura della violazione è ripresa dal Modello di notifica al Garante in caso di data breach, sezione C note al punto 6.

Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).	Medio	2
Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).	Grave	3
Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).	Gravissimo	4

3a. **Perdita di riservatezza (Divulgazione/ accesso non autorizzato o accidentale)**	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.)	☐ 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	
	☐ Perdita di riservatezza dei dati personali protetti da segreto professionale	Rivelazione del segreto professionale (art. 622 c.p.)	
	☐ Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
	☐ altro_____	_____	
3b. **Perdita di integrità** dei dati **(Modifica non**	**Conseguenze** per gli interessati della perdita di integrità dei	Impatto sui **diritti e le libertà** degli interessati:	**Livello di impatto** della perdita di integrità dei dati:

autorizzata o accidentale)	dati:		
	☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ 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	
	☐ Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
	☐ altro_____	_____	
3c. **Perdita di disponibilità** dei dati **(Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale)**	**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
	☐ 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. indicare la **stima della probabilità** di accadimento delle minacce in base alla scala riportata di seguito. Si tratta di una scala di tipo "semi quantitativo", ovvero, la valutazione è guidata dal criterio (espresso in termini qualitativi) che corrisponde al livello (espresso in termini qualitativi) e al valore (espresso in termini numerici).

CRITERIO	LIVELLO	VALORE
• La mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili indipendenti • L'evento non si è mai verificato negli ultimi 5 anni • Il verificarsi del danno conseguente la mancanza rilevata susciterebbe incredulità in azienda	Improbabile	1
• La mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi • L'evento si è verificato negli ultimi 5 anni e/o ci si aspetta una frequenza fra 1 e 3 anni • Il verificarsi del danno conseguente la mancanza rilevata susciterebbe una grande sorpresa in azienda	Poco probabile	2
• La mancanza rilevata può provocare un danno, anche se non in modo automatico o diretto • L'evento si è verificato negli ultimi 3 anni e/o ci si aspetta una frequenza fra 1 mese ed 1 anno • Il verificarsi del danno conseguente la mancanza rilevata susciterebbe una moderata sorpresa in azienda	Probabile	3
• Esiste una correlazione diretta tra la mancanza rilevata e il verificarsi del danno ipotizzato • L'evento si è verificato nell'ultimo mese e/o ci si aspetta una frequenza inferiore a 1 mese • Il verificarsi del danno conseguente la mancanza rilevata susciterebbe alcuno stupore in azienda	Molto probabile	4

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. individuare la **stima dell'impatto** provocato dall'accadimento delle minacce che corrisponde al valore più elevato tra i tre livelli di impatto su ognuno dei tre requisiti di sicurezza calcolati al punto 3

5. Stima dell'impatto (fattore I della formula di calcolo del Rischio)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3

	☐ Gravissimo 4

6. calcolare la gravità del **rischio inerente** incrociando i valori qualitativi che risultano dalla stima della probabilità e dalla stima dell'impatto (R_i=PxI), che possono generare risultati da 1 (impatto lieve e improbabile) a massimo 16 (impatto gravissimo e molto probabile)

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. indicare le **misure di sicurezza tecniche e organizzative** già in atto che contribuiscono a ridurre la probabilità e l'impatto di un evento negativo.

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	inserire le misure di sicurezza già implementate

8. indicare il **livello di adeguatezza delle misure di sicurezza** in base alla scala riportata di seguito.

CRITERIO	LIVELLO
Misure di mitigazione adeguate ai requisiti di legge e capaci di fungere da contromisure rispetto alle tipologie di rischio individuate.	Adeguate
Modalità organizzative e gestionali di sola sufficienza rispetto alle tipologie di rischio individuate e alla conformità legislativa.	Minime
Modalità organizzative e gestionali insufficienti rispetto alle tipologie di rischio individuate e alla conformità legislativa.	Insufficienti

Nessuna previsione di misure di mitigazione nonostante un rischio inerente MEDIO / ALTO / MOLTO ALTO.	Inesistenti

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

9. calcolare la gravità del **rischio residuo** alla luce delle misure in atto, incrociando il livello di adeguatezza delle misure con il livello di gravità del rischio inerente;

9. Stima del rischio residuo

		Misure di sicurezza			
		Adeguate	Minime	Insufficienti	Inesistenti
Ri	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. indicare le **modalità di mitigazione del rischio** per gestire il rischio residuo: solo in caso di rischio basso (1-3) o medio (4-6) è possibile optare per l'accettazione del rischio;

10. Modalità di mitigazione del rischio per gestire il rischio residuo	☐ nessuna: accettazione del rischio (1-3) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____

11. nel caso in cui come modalità di mitigazione del rischio sia stata indicata l'"adozione di ulteriori misure di sicurezza" indicare quali **misure ulteriori di sicurezza** contribuiscono a ridurre la probabilità e l'impatto di un evento negativo.

11. Quali misure ulteriori di sicurezza contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	inserire le misure di sicurezza che si intende implementare per mitigare il rischio

12. indicare **entro quanto tempo** dovranno essere attuate le ulteriori misure di sicurezza sulla base dei valori ottenuti nella tabella di calcolo del rischio residuo

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. indicare la/e **funzione/i aziendale/i** o il/i **responsabile/i di funzione** deputato/i ad attuare le ulteriori misure di sicurezza. È possibile fare riferimento ai soggetti indicati nel paragrafo iniziale "Organizzazione e obiettivo del documento" (CPO, DPO, PM, Legale/CM, CISO, RTD).

13. Responsabile/i dell'attuazione delle ulteriori misure di sicurezza	1. 2.

14. indicare l'**accettabilità del rischio residuo** in base al valore ottenuto nella tabella al punto 9 e alla valutazione qualitativa delle risposte fornite ai punti 10 e 11.

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