Asuit
Azienda Sanitaria Universitaria Integrata del Trentino

Valutazione di impatto sulla protezione dei dati personali

(Estratto)

relativa al progetto di ricerca

Studio osservazionale multicentrico, retrospettivo e prospettico, sulla sicurezza del trattamento radiante adiuvante in pazienti affetti da carcinoma della mammella in terapia con Trastuzumab Emtansine (T-DM1)

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 sanitaria universitaria integrata del Trentino (Asuit)
Titolo dello studio	Studio osservazionale multicentrico, retrospettivo e prospettico, sulla sicurezza del trattamento radiante adiuvante in pazienti affetti da carcinoma della mammella in terapia con Trastuzumab Emtansine (T-DM1).
Codice dello studio	RT-OSS 01-2026
Redattori	Dott.ssa Fiorenza DeRose dott.ssa Paola Zanetti
Verificatore interno	Dott. Emanuele Torri
DPO	Avv. Silvia Stefanelli
Versione	1
Data Revisione	03.09.2026

Asuit
Azienda Sanitaria Universitaria Integrata del Trentino

1. Sommario

1. SOMMARIO 2
2. OBIETTIVO E ORGANIZZAZIONE DEL DOCUMENTO. 3
3. DEFINIZIONE DEL CONTESTO. 5
3.1 ELEMENTI DI FATTO 5
3.2 RUOLI PRIVACY 5
3.3 DESCRIZIONE GENERALE DELL'ATTIVITÀ DI TRATTAMENTO 6
4. RAPPRESENTAZIONE DEL CICLO DI VITA DEI DATI 8
4.1 Fase della raccolta dei dati. *9*
4.2 Fase della archiviazione dei dati. *10*
4.3 Fase dell'accesso ai dati. *10*
4.4 Fase dell'elaborazione dei dati. *12*
4.5 Fase della trasmissione dei dati. *12*
4.6 Fase della conservazione dei dati *14*
4.7 Fase della eliminazione dei dati. *15*
5. CONFORMITÀ ALLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI 16
5.1. Criteri indicativi di rischio elevato *16*
5.2. Rispetto del principio di finalità *16*
5.3. Rispetto del principio di liceità *17*
5.4. Consultazione degli interessati *19*
5.5. Rispetto del principio di trasparenza *19*
5.6. Misure di protezione dei diritti degli interessati *20*
5.7. Rispetto del principio di minimizzazione *20*
5.8. Rispetto del principio di proporzionalità *21*
5.9. Rispetto del principio di esattezza *22*
5.10. Rispetto del principio di limitazione della conservazione *22*
5.11. Soggetti esterni *23*
5.12. Contitolari del trattamento *24*
5.13 Trasferimento dei dati extra UE *25*
6. TABELLE DI CALCOLO DEL RISCHIO E VALUTAZIONE DELL'IMPATTO SUGLI INTERESSATI. 25
6.1. PERDITA DI RISERVATEZZA 27
6.2. PERDITA DI INTEGRITÀ 30
6.3. PERDITA DI DISPONIBILITÀ 33
7. CONCLUSIONI 37
7.1 VALUTAZIONE FINALE 37
7.2 RISCHIO RESIDUO 37

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])

[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).

6. Definizione dei meccanismi dell'eventuale trasferimento dei dati in Paesi 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 sanitaria universitaria integrata del Trentino (di seguito "Asuit") 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 "Studio osservazionale multicentrico, retrospettivo e prospettico, sulla sicurezza del trattamento radiante adiuvante in pazienti affetti da carcinoma della mammella in terapia con Trastuzumab Emtansine (T-DM1)" promosso da Azienda sanitaria universitaria integrata del Trentino (Asuit).

In particolare, il progetto di ricerca consiste nella raccolta ed analisi dei dati sulla sicurezza del trattamento radiante in pazienti con neoplasia della mammllea HER2 positive (HER2+) in terapia con Trastuzumab Emtansine (T-DM1), un anticorpo farmaco-coniugato, al fine di confermare anche in un setting "real world" che il trattamento radiante non si associa ad un significativo incremento degli eventi avversi locali, acuti e tardivi.

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 sanitaria universitaria integrata del Trentino**
SEDE LEGALE	Via Degasperi 79, 38123 Trento
INDIRIZZO MAIL	dirgen@asuit.tn.it
INDIRIZZO PEC	asuit@pec.asuit.tn.it
DPO	responsabileprotezioniondati@asuit.tn.it

b) Contitolari del trattamento

(non applicabile)

c) Responsabili del trattamento

(non applicabile)

3.3 Descrizione generale dell'attività di trattamento

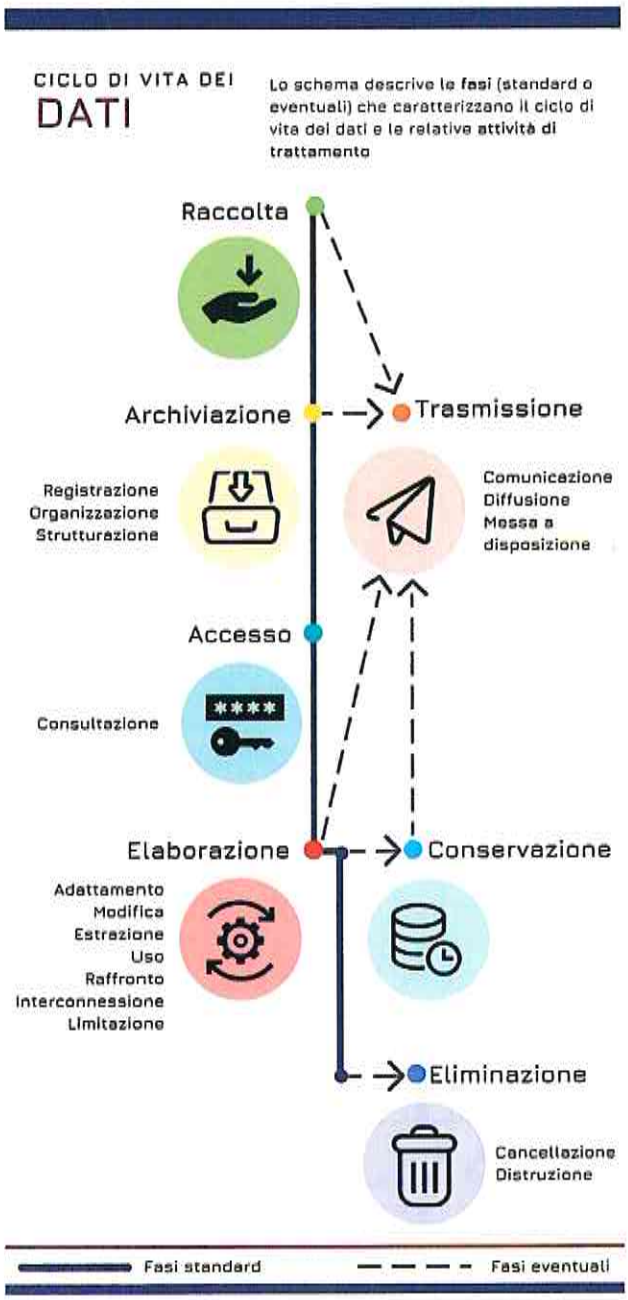
In questo paragrafo sono individuate le caratteristiche generali del progetto.

BREVE DESCRIZIONE DEL PROGETTO DI RICERCA	In assenza di evidenze di livello 1 sul profilo di sicurezza della terapia radiante adiuvante in pazienti con neoplasia della mammella HER2 positive (HER2+) in terapia con Trastuzumab Emtansine (T-DM1), è fortemente raccomandata la raccolta sistematica di dati real-world (retrospettivi e prospettici), comprensivi di dettagli mancanti (specifiche del trattamento radiante erogato in termini di dosi e volumi) negli studi già pubblicati su associazione RT adiuvante e T-DM1. L'obiettivo primario dello studio è la valutazione degli eventi avversi acuti e tardivi locali correlati al trattamento radiante adiuvante in tale sottogruppo di pazienti; l' incidenza e il grado degli eventi avversi saranno registrati secondo la scala di tossicità standardizzata (CTCAE Version 5). Il periodo di arruolamento sarà di due anni complessivi (fino a Dicembre 2028) e i pazienti verranno seguiti in follow up/osservazione per 5 anni complessivi (fino a Dicembre 2033). Allegato n. 1 - **SINOSSI Studio multicentrico real-world RT-OSS 01-2026_v1.0_13.02.2026**
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: Codice Identificativo, Centro di appartenenza, Sesso, Data di nascita, Età alla diagnosi (biopsia), Comorbidità concomitanti, Terapia farmacologica in atto; dati alla diagnosi (lateralità del tumore, stadio clinico, sottotipo molecolare); dettagli relativi ai trattamenti/interventi effettuati (tipo di chirurgia, stadio patologico, volumi, dosi e tecniche relativi al trattamento radiante, numero di cicli di T-DM1, totali e pre-RT); dati relativi a tossicità acuta (</= 6 mesi dal termine della radioterapia) e tardiva (>6 mesi dal termine della radioterapia), con particolare riferimento agli eventi avversi cutanei, polmonari e cardiaci; outcomes clinici di interesse (recidiva locale, recidiva locoregionale, metastasi a distanza, stato di malattia all'ultimo follow up); compilazione dei questionari sulla Qualità di Vita (solo per la parte prospettica); dati relativi alla cosmesi (solo per la parte prospettica) ☐ Altro SPECIFICARE: _____
CONSENSO INFORMATO	Viene prevista l'acquisizione del consenso informato allo studio: X SI 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 22.04.2026 ☐ 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.



(Omissis)

5.13 Trasferimento dei dati extra UE

In questa sezione vengono riportate le basi di legittimità del trasferimento dei dati a soggetti che sono stabiliti in Paesi esterni allo Spazio Economico Europeo (Capo V del GDPR).

TRASFERIMENTO DATI EXTRA UE	
I dati vengono trasferiti al di fuori dell'Unione Europea?	☐ SÌ X NO Se la risposta alla domanda precedente è SI, è stato redatto un Transfer Impact Assessment (valutazione della legittimità del trasferimento)? ☐ SÌ ☐ NO Se la risposta alla domanda precedente è SI, compilare la tabella seguente.

Indicare i Paesi terzi in cui i dati vengono trasferiti	Indicare il contesto e la finalità del trasferimento	Indicare le basi di legittimità del trasferimento

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.

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

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)

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, ransomware, 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 ☐ 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.)	☐ Lieve 1 X 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)	☐ Lieve 1 X 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	X 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 [attribuzione ad ogni soggetto di un codice alfanumerico univoco. Conservazione dell'elenco di collegamento tra codice e identità del paziente esclusivamente presso il centro di arruolamento, sotto la responsabilità del PI] X limitazione degli accessi [*descrizione delle modalità*: accesso consentito solo agli autorizzati con credenziali personali non cedibili_] X Misure di protezione dagli attacchi informatici [misure di protezione in atto in Asuit] X Adozione di una policy per il corretto utilizzo degli strumenti informatici X Formazione del personale ☐ _____

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

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	X 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

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, ransmoware, etc.)
2. Quali sono le principali vulnerabilità	☐ Mancanza di regolarità nella manutenzione

rilevate?	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 ☐ 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)	☐ Improbabile 1 X 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	☐ 1	X 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 X Formazione del personale ☐ 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	X 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

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, 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	☐ basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-

inerente:				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	1.

ulteriori misure di sicurezza	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 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.

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 Delegato al trattamento
dott. Emanuele Torri