Valutazione di impatto
sulla protezione dei dati personali

(estratto)

relativa allo

studio osservazionale "Artificial Intelligence in Digital Pathology in Colon Cancer in the Adenoma-Carcinoma Progression sequence - AIDiP-CC-ACaPro"

ed allo

studio osservazionale "Artificial Intelligence in Digital Pathology in Colon Cancer in Cancer-Stromal-Immune Cell interaction in colonic Adenocarcinoma - AIDiP-CC-CaStICA"

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

Contitolari del trattamento	Azienda sanitaria universitaria integrata del Trentino (Asuit) e Fondazione Bruno Kessler (FBK)
Titolo degli studi studio	• Artificial Intelligence in Digital Pathology in Colon Cancer in the Adenoma-Carcinoma Progression sequence - AIDiP-CC-ACaPro • Artificial Intelligence in Digital Pathology in Colon Cancer in Cancer-Stromal-Immune Cell interaction in colonic Adenocarcinoma - AIDiP-CC-CaStICA
Redattori	• Asuit: prof. dott. Mattia Barbareschi, dott. Alessandro Zorer, dott. Giampaolo Franco • Unita' Data Science for Health di FBK: dott. Matteo Pozzi, dott.ssa Lisa Novello, dott. Flavio Ragni, dott. Stefano Bovo, dott. Shahryar Noei; • Unità Prevenzione della Corruzione, Trasparenza e Privacy di FBK: dott.ssa Anne Elisabeth Beumer; • Project manager per FBK: dott.ssa Jacqueline Marcon
DPO	• avv. Silvia Stefanelli (per Asuit) • dott. Anna Benedetti (per FBK)
Versione	1
Data Revisione	- DPO di FBK: 12/05/2025 - DPO di Asuit: 13/11/2025

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 dei progetti di ricerca analizzati.

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 (ossia dei soggetti 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 contitolari 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 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

[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).

[7] Capo V GDPR.

	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).

[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.

Fondazione Bruno Kessler (di seguito "FBK") ha tra i propri fini istituzionali la promozione della cultura e dell'innovazione e il trasferimento di conoscenze e tecnologie, al fine di contribuire alla crescita della comunità e dell'economia trentina nella quale è radicata. FBK promuove e sviluppa attività di ricerca in vari settori, principalmente negli ambiti delle tecnologie digitali e dell'intelligenza artificiale (industria e salute digitale, cyber security, smart cities), dei sensori, dei dispositivi, delle energie sostenibili, degli studi umanistici, della valutazione delle politiche pubbliche.

La presente DPIA valuta il trattamento dei dati personali nell'ambito dei seguenti due progetti di ricerca:

- lo studio osservazionale *"Artificial Intelligence in Digital Pathology in Colon Cancer in the Adenoma-Carcinoma Progression sequence - AIDiP-CC-ACaPro"* (di seguito lo "**Studio AIDiP-CC-ACaPro**") è promosso da Asuit e FBK. Lo studio AIDiP-CC-ACaPro consiste nello sviluppo di sistemi di intelligenza artificiale volti a migliorare l'accuratezza e l'efficienza nell'identificazione delle lesioni del colon con una particolare attenzione alla sua identificazione precoce. I dati utilizzati dal progetto includono immagini di biopsie del colon digitalizzate. I tessuti utilizzati comprendono mucosa normale, diversi tipi di polipi ed adenocarcinomi. Verranno inoltre integrate immagini endoscopiche e dati clinici dei pazienti. La ricerca ha lo scopo di valutare la fattibilità di una diagnostica digitale e di sviluppare contestualmente algoritmi di intelligenza artificiale in grado di identificare adenocarcinomi del colon, diverse tipologie di polipi e grado di displasia, investigare le relazioni tra lo sviluppo e l'aggressività dell'adenocarcinoma con il tipo di polipi presenti nell'area di interesse. Obiettivo primario dello studio è lo sviluppo e validazione di tali strumenti ai soli fini di ricerca. L'esplorazione di implementazioni cliniche, nonostante siano potenzialmente rilevanti, restano escluse dallo scopo di questo progetto;
- lo studio osservazionale *"Artificial Intelligence in Digital Pathology in Colon Cancer in Cancer-Stromal-Immune Cell interaction in colonic Adenocarcinoma - AIDiP-CC-CaStICA"* (di seguito lo "**Studio AIDiP-CC-CaStICA**") è promosso da Asuit e FBK. Lo studio AIDiP-CC-CaStICA consiste nell'analisi dell'espressione di specifici marcatori delle cellule tumorali e dei sottotipi di fibroblasti associati al cancro e dei sottotipi di cellule immunitarie in una grande coorte di Adenocarcinoma del colon con follow-up a lungo termine (> 5 anni). Nello specifico, verrà studiata l'interazione tra le cellule tumorali con il microambiente tumorale circostante, con particolare attenzione alla gemmazione tumorale (tumor budding) con l'obiettivo di identificare marcatori prognostici/predittivi rilevanti. Verranno utilizzati dati clinici dei soggetti e vetrini istologici digitalizzati trattati con immunocolorazioni multiple per i marcatori di interesse e con tecniche immunoistochimiche, per la co-localizzazione di biomarcatori selezionati a livello cellulare. L'analisi dei dati, effettuata a scopo di ricerca, sarà affidata ad algoritmi di intelligenza artificiale (IA) uni e multi modali che verranno sviluppati appositamente per tale scopo.

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

Non applicabile

b) Contitolari del trattamento

CONTITOLARI DEL TRATTAMENTO		
	CONTITOLARE 1	**CONTITOLARE 2**
RAGIONE SOCIALE	Azienda sanitaria universitaria integrata del Trentino (Asuit)	Fondazione Bruno Kessler (FBK)
SEDE LEGALE	Trento, CAP 38123, Via Alcide Degasperi n. 79	Trento, CAP 38122, via Santa Croce n. 77
INDIRIZZO MAIL	dirgen@asuit.tn	privacy@fbk.eu
INDIRIZZO PEC	asuit@pec.asuit.tn.it	privacy@pec.fbk.eu
DPO	Avv. Silvia Stefanelli	Dott.ssa Anna Benedetti

c) Responsabili del trattamento

RESPONSABILE DEL TRATTAMENTO	
RAGIONE SOCIALE	Trentino Digitale
SEDE LEGALE	Via G. Gilli, 2 - 38121 Trento
INDIRIZZO MAIL	tndigit@tndigit.it
INDIRIZZO PEC	tndigit@pec.tndigit.it
DPO	Avv. Massimo Melica - dpo@tndigit.it
Quale Contitolare ha provveduto alla nomina ex art. 28 GDPR	Asuit

RESPONSABILE DEL TRATTAMENTO	
RAGIONE SOCIALE	Trentino AI Scarl
SEDE LEGALE	Via Kufstein, 5 - 38121 Trento

INDIRIZZO MAIL	info@trentino.ai
INDIRIZZO PEC	trentinoai@pec.it
DPO	privacy@deltainformatica.eu
Quale Contitolare ha provveduto alla nomina ex art. 28 GDPR	Asuit

RESPONSABILE DEL TRATTAMENTO	
RAGIONE SOCIALE	Deda Next Spa
SEDE LEGALE	Via di Spini 50 - 38121 Trento
INDIRIZZO MAIL	info@dedagroup.it
INDIRIZZO PEC	deda.next@legalmail.it
DPO	dpo@dedagroup.it
Quale Contitolare ha provveduto alla nomina ex art. 28 GDPR	Asuit

RESPONSABILE DEL TRATTAMENTO	
RAGIONE SOCIALE	iConsulting Spa
SEDE LEGALE	Casalecchio di Reno (BO), via Bazzanese 32/7
INDIRIZZO MAIL	dpo@iconsulting.biz, info@iconsulting.biz
INDIRIZZO PEC	iconsultingspa@legalmail.it
DPO	dpo@iconsulting.biz
Quale Contitolare ha provveduto alla nomina ex art. 28 GDPR	Asuit

3.3 Descrizione generale dell'attività di trattamento

In questo paragrafo sono individuate le caratteristiche generali del progetto.

BREVE DESCRIZIONE DEI PROGETTI DI RICERCA	• **Per lo Studio AIDiP-CC-ACaPro: Allegato 2a** • **Per lo Studio AIDiP-CC-CaStICA: Allegato 2b**
TIPO DI RICERCA	**x Studio unicentrico** ☐ Studio multicentrico ☐ 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: rapporto istologico, immagini endoscopiche e referto, set di dati clinici **x Altro** SPECIFICARE: **campioni biologici e istologici**
CONSENSO INFORMATO	Viene prevista l'acquisizione del consenso informato allo studio: **x SI, salvo nell'eventualita' in cui questo risulti impossibile** ☐ NO
COMITATO ETICO	Il progetto di ricerca ha ottenuto motivato parere favorevole dal competente Comitato Etico a livello territoriale? **x SÌ, parere di data _04/12/2025** ☐ NO ☐ in corso di sottomissione

Omissis

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.

---

[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)

- 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 6.1., 6.2. e 6.3. deve seguire le istruzioni riportate nell'**Allegato 1**.

6.1. Perdita di riservatezza

Perdita di riservatezza	La perdita di riservatezza dei dati non ha impatto sui diritti e le libertà degli interessati? X SI, in caso di perdita di riservatezza ci sarebbero conseguenze sui diritti e le libertà degli interessati > 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 X Intercettazione del traffico Ethernet non cifrato; acquisizione dei dati inviati su una rete Wi-Fi, X Condivisione dei dati con soggetti non autorizzati X Recupero illegittimo delle chiavi di pseudo-anonimizzazione dei dati X Penetrazione al sistema di pseudononimizzazione ☐ _____
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 ☐ Trasferimento dati in chiaro (senza cifratura) ☐ Salvataggio dati in chiaro (senza cifratura) X Non sono state rilevate vulnerabilità	
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 ☐ Medio 2 ☐ Grave 3 X Gravissimo 4
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
X Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
X Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
X Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
X 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 ☐ Medio 2 ☐ Grave 3 X Gravissimo 4	
6. **Rischio inerente** (R = P x I)		
P		

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

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

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	X crittografia [descrizione delle tecniche di crittografia:_____] X pseudonimizzazione [*descrizione delle tecniche di pseudonimizzazione*: descrizione disponibile nell'**allegato 3** X limitazione degli accessi [*descrizione delle modalità*: descrizione disponibile nell'**allegato 3**] X misure di protezione dagli attacchi informatici [*descrizione delle misure*: descrizione disponibile nell'**allegato 3**] 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)o

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?	• N/A
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) N/A
13. Responsabile/i dell'attuazione delle ulteriori misure di sicurezza	1.N/A

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 non ha impatto sui diritti e le libertà degli interessati? X SI, in caso di perdita di integrità ci sarebbero conseguenze sui diritti e le libertà degli interessati > compilare il paragrafo 6.2 ☐ NO > passare al paragrafo 6.3

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?	X Malfunzionamento dell'hardware X Malfunzionamento del software ☐ Deterioramento degli strumenti informatici X Errore umano nell'inserimento dei dati X Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet X Attacco deliberato interno o esterno

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 ☐ Mancata formazione del personale X Non sono state rilevate vulnerabilità	
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)o

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 X Antivirus, procedure awareness, Intrusion detection etc. (vedere tabella su Riservatezza)

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)o

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?	• N/A
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) N/A
13. Responsabile/i dell'attuazione delle ulteriori misure di sicurezza	N/A

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 non ha impatto sui diritti e le libertà degli interessati? ☐ SI > compilare il paragrafo 5.3 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.)	x 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
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 ☐ 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)o

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)o

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 Pareri dei DPO

Parere del DPO di FBK del 12 maggio 2025:

Nella redazione della presente DPIA sono state rappresentate in modo chiaro tutte le fasi del ciclo di vita dei dati trattati da ciascun Contitolare e sono state valutate le condizioni che assicurano il rispetto di tutti i principi dettati dal GDPR.

I potenziali rischi per i diritti e le libertà delle persone fisiche interessate individuati dai Contitolari sono stati valutati in termini di probabilità e gravità del danno attraverso una ricognizione delle misure tecniche ed organizzative di mitigazione degli stessi. Tali misure risultano adeguate a garantire la conformità del trattamento al GDPR.

Nel confronto con i redattori interni, la DPO FBK ha inserito i propri commenti direttamente nella documentazione durante la propria revisione e, sulla base di tutte le informazioni ricevute, approva ufficialmente la presente DPIA fornendo, al contempo, le seguenti raccomandazioni ai Contitolari del trattamento:

- dare puntuale attuazione alle misure di mitigazione individuate e monitorarne periodicamente lo stato di attuazione;
- vigilare sul rispetto delle istruzioni fornite ai soggetti autorizzati al trattamento e ai soggetti esterni nominati quali Responsabili del trattamento;
- coinvolgere le rispettive Unità Privacy in caso di modifiche significative ai trattamenti oggetto della presente DPIA.

Parere del DPO di Asuit del 13 novembre 2025:

Il DPO ha valutato la presente valutazione di impatto e l'ha ritenuta conforme all'art. 35 GDPR e alle Linee guida del Gruppo di lavoro ex art. 29.

Dalle valutazioni svolte è risultato che i Contitolari- tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché delle probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche - mettono in atto misure tecniche e organizzative che sono ritenute adeguate a garantire che il trattamento è effettuato conformemente al Regolamento UE 2016/679.

Considerate le misure di sicurezza in atto nel trattamento di dati oggetto della presente DPIA, non si rilevano condizioni di rischio residuo elevato e, pertanto, non è necessario consultare l'Autorità garante ai sensi dell'art. 36 del GDPR.

Si raccomanda di riesaminare periodicamente e ad aggiornare, se necessario, la presente valutazione d'impatto.

7.2 Valutazione finale

I Contitolari 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, mettono 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 e 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 il soggetto 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 per la mitigazione del rischio.

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

7.3 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*)".

I Contitolari hanno 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.

I Contitolari del trattamento

Azienda sanitaria universitaria integrata del Trentino
Il Direttore Generale, dott. Antonio Ferro

_____

Fondazione Bruno Kessler,
nella persona del direttore del Centro Digital Health & Wellbeing,
dott. Federico Cabitza

_____

Omissis