Valutazione di impatto
(*data protection impact assessment* - DPIA)
sulla protezione dei dati personali

redatta ai sensi dell'art. 35 del Reg. UE 679/2016 e sulla base delle Linee Guida del 4/10/2017 del Working Party Art. 29.

CONSORZIO FUTURO IN RICERCA

DATA EMISSIONE	13/05/2024
REDATTORE	DOTT. G. MONTECCHIO
VERIFICATORE INTERNO	DOTT.SSA M. SIVIERI
VALIDATORE	PROF. D. VINCENZI
VERSIONE	1.0.
DATA REVISIONE	

DOCUMENTO PUBBLICATO PER ESTRATTO PER RAGIONI DI TUTELA DELLA PROPRIETA' INTELLETTUALE

Il documento può essere consultato integralmente su istanza dell'interessato da formulare al Titolare agli indirizzi
PEO: cfr@unife.it
PEC: cieffeerre@pec.it

PROBABILITÀ					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	*(1 ≤ Ri ≤ 2)*
Basso	*(3 ≤ Ri ≤ 4)*
Rilevante	*(6 ≤ Ri ≤ 9)*
Alto	*(12 ≤ Ri ≤ 16)*

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- **0,25;**
- **0,5;**
- **1.**

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia ALTA, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Modalità di elaborazione dati: Informatica	
Strumenti	**Applicativi Microsoft Office 365 e Google Workspace**
Strutture informatiche di archiviazione	**Il software viene installato su hardware del Cliente. La parte cloud è su sistemi Cloud Microsoft e Google**
Strutture informatiche di backup	**Vengono effettuati regolarmente backup**

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	**Marginali**	**Medio-basso**

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Il modulo CRF è un Excel cifrato **- Sono gestiti i back up** **- Vengono registrati e conservati i Log file** **- Viene eseguita una regolare formazione del personale**

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
E' applicata una gestione della password degli utenti	• **Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)** • **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** • **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)**	**Adeguate**
E' presenta una politica per la sicurezza e la protezione dei dati	• **Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)** • **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** • **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)**	**Adeguate**

I dati sono crittografati	• **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** • **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)**	**Adeguate**
Le password sono modificate al primo utilizzo	• **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** • **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)**	**Adeguate**
Le password sono modificate ogni 3 mesi	• **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** • **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)**	**Adeguate**
Sono gestiti i back up	• **Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)** • **Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)** • **Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)** • **Agenti fisici (incendio, allagamento, attacchi esterni)**	**Adeguate**
Vengono registrati e conservati i Log file	• **Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)** • **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)**	**Adeguate**
Viene eseguita una regolare formazione del personale	• **Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)**	**Adeguate**

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)
RISCHI
• Perdita • Distruzione non autorizzata

• **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	**Trascurabili**	**Molto basso**
VALUTAZIONE RISCHIO NORMALIZZATO ***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi***		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Molto basso	**0,25**	**Molto basso**

PERICOLO
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
RISCHI
• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata** • **Divulgazione non autorizzata** • **Accesso dati non autorizzato**

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	**Trascurabili**	**Molto basso**
VALUTAZIONE RISCHIO NORMALIZZATO ***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi***		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Molto basso	**0,25**	**Molto basso**

PERICOLO
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
RISCHI
• **Perdita** • **Distruzione non autorizzata** • **Modifica non autorizzata**

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	**Trascurabili**	**Molto basso**
VALUTAZIONE RISCHIO NORMALIZZATO ***Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi***		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Molto basso	**0,25**	**Molto basso**

A valle dell'aggiornamento della DPIA, il trattamento risulta a rischio Molto basso