Valutazione di impatto sulla protezione dei dati

In ottemperanza degli articoli 32, 35 e 36 del Regolamento generale sulla protezione dei dati

Versione	Mese Anno	Note
1.0	Luglio 2025	

Sommario

Titolare del trattamento

Ragione Sociale	SYNLAB SDN S.r.l.	
P.IVA	01288650631	
Sede legale	Via Francesco Crispi 8 - NAPOLI	
Legale rappresentante	Fabio Tedeschi	
PEC	sdnspa@pec-sdn-napoli.it	
Responsabile della Protezione dei dati	SYNLAB Italia Srl	privacy@synlab.it

Finalità del documento

Il presente documento è finalizzato alla rappresentazione delle analisi sostenute in materia di sicurezza nel trattamento dei dati personali: in particolare, viene rappresentata

- La descrizione sistematica del trattamento
- l'analisi dei rischi sul trattamento,
- la determinazione delle misure di sicurezza, tecniche e organizzative, adeguate per garantire un livello di sicurezza adeguato al rischio
- la conduzione di una valutazione di impatto sulla protezione dei dati

Soggetti coinvolti

ENTE	NOME E COGNOME	FUNZIONE	ATTIVITÀ
SYNLAB Italia S.r.l.	Ettore Gendusa	DPO	• Supervisione all'intero ciclo di conduzione della valutazione di impatto.
Synlab SDN S.r.l..	Marco Aiello	Referente di ricerca	• Individuazione e analisi sistematica del trattamento • Valutazione della necessità di conduzione della valutazione di Impatto • Descrizione sistematica del trattamento • Individuazione delle minacce e degli impatti sui diritti e sulle libertà degli interessati
Synlab SDN S.r.l..	Fabio Tedeschi	Legale rappresentante	• Analisi dello stato dell'arte • Approvazione dell'esito della valutazione.

Trattamento in esame

- **Trattamento di dati personali strumentale all'attuazione del Progetto "*DIADEMA: Un nuovo workflow neuroradiologico per la diagnosi assistita e la gestione della demenza con l'intelligenza artificiale*"**

Verifica preliminare per l'applicabilità di una DPIA

Sulla base dell'elenco individuato dell'Autorità Garante per la protezione dei dati personali

L'autorità nazionale di controllo, in applicazione dell'art.35, comma 5 del Regolamento Generale sulla Protezione dei Dati ha reso pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

Di seguito viene data segnalazione delle attività di trattamento oggetto della presente analisi che sono compatibili con i trattamenti individuati dall'Autorità Garante per la protezione dei dati personali.

☐	Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato
☐	Trattamento automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere
☐	Trattamenti che prevedono utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadata ad es. in ambito telecomunicazioni, banche ecc.. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
☐	Trattamenti su larga cala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
☐	Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti
☐	Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
☐	Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati dispositivi *wearable*¸ tracciamenti di prossimità come ad es. il Wi-Fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248 rev01
☐	Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
☐	Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (mobile payment)
X	Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penale e a reati di cui allart.10 interconnessi con altri dati personali raccolti per finalità diverse
☐	Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
☐	Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

Sulla base dei nove criteri individuati dal Gruppo di Lavoro Articolo 29

Il Gruppo di lavoro ritiene necessaria la conduzione di una Valutazione d'impatto qualora un trattamento soddisfi almeno due dei nove criteri individuati, e di seguito indicati.

☐	Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;
☐	processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29
☐	monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c)). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);
X	dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;
☐	trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala16: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento;
☐	creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
X	dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;
☐	uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;
☐	quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

Esito

Tenuto conto delle attività di trattamento individuate dall'Autorità Garante per la protezione dei dati personali e delle linee guida del Gruppo di Lavoro articolo 29, il Trattamento di dati personali strumentale all'attuazione del Progetto "Definizione, valutazione e condivisione di metodologie per il controllo qualità in diagnostica per immagini" può presentare un rischio elevato per i diritti e le libertà dei soggetti interessati e si rende necessaria la conduzione di una valutazione di impatto.

Descrizione sistematica del trattamento

Finalità del trattamento	Ricerca scientifica
Descrizione	Studio osservazionale multicentrico retrospettivo e prospettico ***Per implementare un sistema innovativo per il miglioramento del workflow neuroradiologico per lo studio della demenza con l'impiego di tecniche di intelligenza artificiale, condotto presso l'IRCCS SYNLAB SDN in collaborazione con L'Università di Roma Tor Vergata, l'IRCCS Centro San Giovanni di Dio Fatebenefratelli e l'Università di Napoli Federico II.***
Soggetti interessati del trattamento	- Pazienti IRCCS SYNLAB - Pazienti delle unità cliniche (UC) aderenti al progetto
Dati trattati	**PAZIENTI IRCCS SYNLAB SDN** - Nome, cognome e altri elementi di identificazione personale - Esami diagnostici relativi alle modalità di imaging (RX, CT, MR, PET, SPECT), - distretti corporei su cui siano disponibili immagini diagnostiche in formato DICOM, - dati anamnestici, - quesito clinico - referto **PAZIENTI DELLE UC ADERENTI AL PROGETTO** Tali informazioni sono trattati previa pseudononimizzazione effettuata da parte di ciascuna unità clinica aderente al Progetto. IRCCS SYNLAB SDN non è in grado di risalire all'identità di tali pazienti. - Esami diagnostici relativi alle modalità di imaging (RX, CT, MR, PET, SPECT), - distretti corporei su cui siano disponibili immagini diagnostiche in formato DICOM, - dati anamnestici, - quesito clinico - referto **DATI PUBBLICI condivisi per scopi di ricerca**
Base giuridica del trattamento	- I dati saranno trattai sulla sulla base del combinato disposto degli artt. 9, par.2 lett. h) del GDPR e dall'art. 110-bis, comma 4, del Codice. Infatti, essendo il Titolare qualificato come Istituto di Ricovero e Cura a Carattere Scientifico (IRCCS) ai sensi del Decreto Legislativo n. 200/2022, ossia "ente a rilevanza nazionale dotato di autonomia e personalità giuridica che, secondo standard di eccellenza, persegue finalità di ricerca, prevalentemente clinica e traslazionale, nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari, unitamente a prestazioni di ricovero e cura di alta specialità", le attività di ricerca vanno ritenute come implicite, secondo quanto previsto per gli IRCCS dall'art. 110-bis, comma 4 del Codice, nei trattamenti effettuati per finalità di diagnosi e cura;

Dati appartenenti a categorie particolari	- Esami diagnostici relativi alle modalità di imaging (RX, CT, MR, PET, SPECT), distretti corporei su cui siano disponibili immagini diagnostiche in formato DICOM, - dati anamnestici, - quesito clinico - referto

Condizione di liceità	- Art. 9, comma II lett.h GDPR, Art. 110-bis comma 4 Codice della Privacy
Dati relativi a condanne penali e reati	Non trattati
Condizione di liceità	N.A.
Necessità e proporzionalità	I dati raccolti sono considerati necessari per l'implementazione del Progetto e l'assenza di uno o più informazioni sopramenzionate possono comportare il mancato raggiungimento degli obiettivi del Progetto di ricerca
Modalità di acquisizione dei dati	- Raccolti direttamente dall'interessato durante il percorso di diagnosi e cura presso l'IRCCS SYNLAB SDN - Forniti da ciascuna unità clinica afferente al Progetto di ricerca, che li ha raccolti presso l'interessato durante il percorso di diagnosi e cura.
Presenza di informativa per gli interessati	- Pubblicata online
Asset coinvolti	- sistemi di elaborazione dati sviluppati "ad hoc" durante il progetto

Altri Stakeholder	- Università di Roma Tor Vergata - IRCCS Centro San Giovanni di Dio Fatebenefratelli - Università di Napoli Federico II.

Autorizzati all'accesso ai dati	• Investigatori del progetto • Collaboratori di ogni centro coinvolto nel progetto • Ricercatori per l'analisi di statistiche aggregate
Destinatari dei dati	I dati grezzi non saranno trasmessi a soggetti terzi al Progetto
Trasferimenti EXTRA-UE	Non previsti
Periodo di conservazione	Fino al termine della fase di disseminazione del progetto (FINE DICEMBRE 2030)

Misure tecniche e organizzative a protezione dei dati personali

TIPOLOGIA	MISURA DI SICUREZZA	implementata	non implementata	non applicabile	pianificata	COMMENTI
PROGETTO DI RICERCA	Account nominativi	X				
	Implementazione della pseudonimizzazione a monte della attività effettuata direttamente da ciascuna SD	X				
EDIFICI	Sistema di allarme	X				
	Sistema di videosorveglianza	X				
	Società di vigilanza notturna/diurna		X			
	Sistema antincendio	X				
	Sistema di autorizzazione per l'accesso ai piani tramite badge	X				
UFFICI	Documenti archiviati in armadi o cassetti muniti di chiave	X				
	Chiave degli armadi o cassetti assegnata esclusivamente al personale preposto	X				
	Distruzione dei fascicoli mediante tritarifiuti	X				
	Distruzione dei fascicoli mediante fornitore certificato per le procedure di scarto documentale	X				
DISPOSITIVI	Stampanti nei corridoi dotate di PIN o *token* per l'avvio della stampa	X				
	Divieto di utilizzo di dispositivi privati per l'archiviazione	X				
POLICY	Regolamenti aziendali per l'archiviazione e la distruzione dei documenti	X				
	Regolamenti aziendali per gli accessi ai locali dell'organizzazione	X				
	Policy aziendali per l'utilizzo della posta elettronica	X				
	Policy aziendali per l'utilizzo delle risorse informatiche	X				
	Formazione del personale in *legal compliance*	X				
SALA SERVER	Accesso ai locali mediante dispositivo (*badge-token*) assegnato al solo personale autorizzato	X				
	Area sottoposta a videosorveglianza	X				
	L'area è inaccessibile al cliente-utente-fornitore	X				
	È Implementato un sistema di autenticazione centralizzato	X				

TIPOLOGIA	MISURA DI SICUREZZA	implementata	non implementata	non applicabile	pianificata	COMMENTI
SISTEMI INFORMATIVI	Sono implementate politiche per la garanzia della complessità e lunghezza delle password	X				
	Impedimento riutilizzo della password	X				
	Tracciamento Autenticazioni degli Amministratori di Sistema	X				
	Profili di autorizzazione differenziati degli utenti per l'accesso ai dati	X				
	Implementati meccanismi di controllo periodico delle autorizzazioni di accesso ai dati	X				
	Procedure di backup	X				
	Cifratura dei backup fuori sede	X				
	Verifica dell'esito positivo delle procedure di backup ad ogni salvataggio	X				
	Sono definite e collaudate periodicamente a campione procedure di ripristino e sono valutati i relativi tempi di attuazione	X				
	Presenza soluzione antivirus regolarmente aggiornato	X				
	Implementati meccanismi di controllo dell'aggiornamento	X				
	Verifica della configurazione di almeno 1 scansione settimanale	X				
	Rete wireless ospiti separata dalla rete interna	X				
	Rete protetta da firewall con funzionalità *web content filtering,* di antivirus di rete, di intrusion prevention / intrusion detection.	X				
	Controllo periodico dell'aggiornamento delle licenze	X				
	Revisione periodica regole di filtraggio	X				
	Sistemi Operativi regolarmente aggiornati	X				
	Software Applicativi c.d. *general purpose* regolarmente aggiornati sulla base della disponibilità degli aggiornamenti del fornitore	X				
	Divieto di installazione software da parte dell'utente	X				
	Cifratura dei volumi dei *device* mobili	X				
	Cifratura dei volumi delle *workstation* fisse		X			
	Mobile Device Management – verifica impostazioni di sicurezza		x			

TIPOLOGIA	MISURA DI SICUREZZA	implementata	non implementata	non applicabile	pianificata	COMMENTI
	Autenticazione a 2 fattori per applicativi Cloud					
	Cifratura del traffico di rete	X				
	Business Application (Gestionali aziendali) regolarmente aggiornate sulla base della disponibilità degli aggiornamenti del fornitore	X				
	Contratto di assistenza per la manutenzione	X				
	protocollo https per l'interazione con la piattaforma	X				
	crittografia dei database della piattaforma	X				

Misure tecniche e organizzative a protezione dei dati personali del fornitore

Valutazione dei rischi e degli impatti

Nella presente sezione, viene effettuata una analisi e valutazione dei rischi per i diritti e le libertà delle persone fisiche nell'ambito del trattamento oggetto di valutazione. I rischi possono derivare qualora il trattamento sia suscettibile "*…di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo […]*"[1].

La valutazione delle probabilità e di accadimento della minaccia, nonché delle possibili conseguenze, viene effettuata falle funzioni LEGAL, SISTEMI INFORMATIVI, dal Direttore della funzione competente del trattamento (ove necessario con il supporto dei propri collaboratori), e con il supporto del Responsabile della Protezione dei dati.

Legenda Probabilità di accadimento (P)

Punteggio	Livello	Descrizione
5	**Alta**	È altamente probabile che l'evento si verifichi più volte nell'arco dell'anno
4	**Probabile**	L'evento può occorrere nel breve periodo (da 1 a 11 mesi)
3	**Possibile**	Può accadere che l'evento si verifichi sul lungo periodo (da 1 a 3 anni)
2	**Improbabile**	Eventi di questo tipo sono rari, ma esiste la possibilità che si verifichino
1	**Raro**	Sebbene possa materialmente accadere, non è ragionevole ipotizzarne l'accadimento

Legenda Impatti sull'interessato (I)

Punteggio	Livello	Descrizione
5	**Estremo**	La violazione dei dati causerebbe gravi conseguenze nei confronti del soggetto interessato, che vede compromesse le proprie libertà o i propri diritti (Interventi, diagnosi o anamnesi cliniche rimandate, privazione della libertà personale,). Sono coinvolti dati appartenenti a categorie particolari e/o relativi a condanne penali e reati.
4	**Significativo**	La violazione dei dati comporterebbe importanti conseguenze nei confronti del soggetto interessato (Discriminazione sul posto di lavoro sulla base di opinioni politiche, abitudini sessuali, informazioni su condanne e reati di familiari e conoscenti - danni reputazionali relativi alle informazioni sullo stato di salute proprio o dei familiari, sulle abitudini sessuali e la vita sessuale, sulle opinioni politiche o l'appartenenza sindacale) Non sono necessariamente coinvolti dati appartenenti a categorie particolari e/o relativi a condanne penali e reati
3	**Moderato**	La violazione dei dati comporterebbe alcune conseguenze nei confronti del soggetto interessato (scherno, allusioni, diffamazione,) non sono coinvolti dati appartenenti a categorie particolari e relativi a condanne penali e reati.
2	**Lieve**	La violazione comporterebbe trascurabili impatti sull'interessato che non causano conseguenze sui diritti e le libertà fondamentali
1	**Insignificante**	La violazione dei dati non è causa di alcuna conseguenza nei confronti dell'interessato

[1] RGPD 2016/679, Considerando n° 75

Legenda Valore di rischio (R)

Punteggio	Livello	Conseguenze
25	**Rischio elevato**	Interruzione dell'attività di trattamento Mitigazione del rischio
da 16 a 20	**Rischio medio-alto**	Rischio mitigabile con azioni correttive da pianificarsi nel breve termine (1-3 mesi)
Da 9 a 12	**Rischio medio-basso**	Rischio mitigabile con azioni correttive pianificabili nel medio lungo termine (1 anno)
da 6 a 8	**Rischio basso**	nessuna ulteriore azione necessaria
da 1 a 5	**Rischio estremamente basso**	nessuna ulteriore azione necessaria

Determinazione del valore di rischio

(Valore di rischio) = (Probabilità di accadimento) * (Impatto sull'interessato)

$$R = P * I$$

		(I) IMPATTO				
		Estremo	**Significativo**	**Moderato**	**Lieve**	**Insignificante**
(P) PROBABILITÀ	**Alta**	**25**	**20**	**15**	**10**	**5**
	Probabile	**20**	**16**	**12**	**8**	**4**
	Possibile	**15**	**12**	**9**	**6**	**3**
	Improbabile	**10**	**8**	**6**	**4**	**2**
	Scarsa	**5**	**4**	**3**	**2**	**1**

Analisi

Minaccia	Descrizione	Rischio per diritti e libertà degli interessati			Note
		P	I	R	Commento
RISERVATEZZA	Divulgazione dei dati personali o accesso agli stessi derivanti da • Errore umano (invio a destinatari errati, abbandono dispositivi, smarrimento *badge*/chiave di accesso, errata configurazione)	2	4	**8**	
	Divulgazione dei dati personali o accesso agli stessi derivanti da • Sabotaggio/Abuso (del personale e/o del fornitore autorizzati)	1	4	**4**	
	Divulgazione dei dati personali o accesso agli stessi derivanti da • Malfunzionamento dei sistemi informativi	1	4	**4**	
	Divulgazione dei dati personali o accesso agli stessi derivanti da • Sottrazione (furto, accesso abusivo, *malware, Cyber*-attacchi)	2	4	**8**	
INTEGRITÀ	Compromissione dei dati a seguito di • Errore umano (utilizzo improprio dei sistemi, confusione documentale, imperizia)	1	1	**1**	La perdita dell'integrità può provocare la compromissione del progetto di ricerca ma senza impatti sugli interessati
	Compromissione dei dati a seguito di • Sabotaggio (del personale e/o del fornitore autorizzati)	1	1	**1**	
	Compromissione dei dati a seguito di • Alterazione (accesso abusivo, *malware, Cyber*-attacchi)	1	1	**1**	

	Compromissione dei dati a seguito di • Malfunzionamento dei sistemi informativi	1	1	**1**	
DISPONIBILITÀ	Distruzione o perdita dei dati personali derivante da • Sabotaggio (del personale e/o del fornitore autorizzati)	1	1	**1**	La perdita della disponibilità può provocare la compromissione del progetto di ricerca ma senza impatti sugli interessati
	Distruzione o perdita accidentali o non autorizzati di dati personali derivante ad esempio da • Disastri naturali climatici/geologici/idrici	1	1	**1**	
	Distruzione o perdita accidentali o non autorizzati di dati personali derivante ad esempio da • Incendio/allagamento	1	1	**1**	
	Distruzione o perdita accidentali o non autorizzati di dati personali derivante ad esempio da • Danneggiamento	1	1	**1**	
	Distruzione o perdita accidentali o non autorizzati di dati personali derivante ad esempio da • Errori di manutenzione	1	1	**1**	
	Distruzione o perdita accidentali o non autorizzati di dati personali derivante ad esempio da • Cyber-attacchi	1	1	**1**	

Esito della valutazione

All'esito delle analisi sostenute il trattamento in esame comporta un livello di **rischio basso** nell'ambito della riservatezza delle informazioni

Essendosi determinato il predetto valore di rischio **pertanto non sussistono elementi di criticità tali da considerare elevato il rischio per le libertà e i diritti delle persone interessate.**

01/07/2025

Referente di ricerca

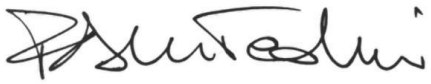
Valutazione complessiva degli impatti sui diritti e le libertà degli interessati

Tenuto conto

- delle considerazioni delle funzioni coinvolte alla conduzione della valutazione
- dei rischi per diritti e le libertà delle persone fisiche derivanti dalle attività di trattamento oggetto della presente analisi
- degli impatti che una violazione dei dati personali potrebbe comportare nei confronti degli interessati,
- della probabilità di accadimento di una violazione di dati personali,
- delle misure tecniche e organizzative attualmente implementate per garantire un livello di sicurezza proporzionato,
- della necessità e proporzionalità del trattamento.

La conduzione della valutazione di impatto ha avuto esito positivo essendosi determinato un valore di rischio basso. Non sussistendo ulteriori elementi di criticità si considera concluso l'iter della valutazione di impatto.

Resta fermo che la presente sarà comunque sottoposta a revisione secondo gli standard aziendali.



Il legale rappresentante