Valutazione di impatto sulla protezione dei dati
DPIA integrativa

Titolare del trattamento	**Azienda ULSS 3 SERENISSIMA** Via Don Federico Tosatto 147 30174, Venezia Mestre C.F. 02798850273 azienda.sanitaria@aulss3.veneto.it
Rappresentante legale	Direttore Generale

DPO	Cervato Law & Business S.r.l. Società tra Avvocati Galleria Europa 3 35137 Padova cervato.sta@pec.it rpd@aulss3.veneto.it

Nome del trattamento	Studio real-world sull'efficacia e la safety della combinazione pembrolizumab-Lenvatinib in pazienti con carcinoma endometriale avanzati in Italia (Reality)

Centro locale di sperimentazione	**UOC Oncologia ospedale di Mirano**

Data DPIA	22/07/2026

Linee Guida	art. 35 GDPR
	Rif. Guidelines WP29 (EDPB) 248/2017
	Rif. Provv. Garante n. 467 11/10/2018
	Template DPIA EDPB

Versione Template DPIA 2026.07

0. Premessa e Contesto di applicazione della DPIA.

L'**art. 35 del Regolamento (UE) 2016/679** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla circolazione di tali dati (""GDPR""), dispone che, quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (""DPIA"" = Data Protection Impact Assessment).
Una singola DPIA può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
La presente DPIA deve intendersi integrativa rispetto alla DPIA già svolta dal Centro Promotore e rispetto alla DPIA generale già svolta dall'Ente per l'ambito della Ricerca (vedi meglio sezione ""Contesto"").
Il titolare del trattamento, allorquando svolge una DPIA, si consulta con il Responsabile della Protezione dei Dati (RPD/DPO), qualora ne sia designato uno.
La DPIA è richiesta nei casi previsti dall'art. 35 par. 3 GDPR, nonché per l'Italia dal provvedimento del Garante n. 467 del 11/10/2018, come previsto dall'art. 35 par. 4 GDPR, come qui sotto descritto.
La DPIA contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40 GDPR.
Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.
Qualora la DPIA indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, il titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di Controllo (Garante per la protezione dei dati personali in Italia).
La presente DPIA viene svolta in quanto, tra le varie ipotesi per cui essa è richiesta in forza dell'art. 35 par. 3 GDPR e del provvedimento del Garante n. 467 del 11/10/2018, si ritiene sussistente almeno quella individuata nel provvedimento suddetto al n. 6: Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo), senza pregiudizio della sussistenza di ogni altra in considerazione, ad esempio, della qualifica di ""larga scala"" del trattamento eseguito (cfr. art. 35 par. 3 GDPR e provvedimento Garante suddetto).
La sussistenza di tale ipotesi è considerata sufficiente e necessaria per la conduzione della presente DPIA.

Art. 35 par. 3 GDPR	Check	Note
Viene svolto un trattamento, **su larga scala**, di categorie particolari di dati personali di cui all'art. 9, par. 1, o di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR	NO	

Art. 35 par. 4 GDPR - All. 1 provv. Garante n. 467 11/10/2018 [doc. web n. 9058979]	Check	Note
4. **Trattamenti su larga scala** di dati aventi carattere estremamente personale (v. WP 248, rev. 01): 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)	NO	
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)	SI	
7. Trattamenti effettuati attraverso l'**uso di tecnologie innovative**, anche con particolari misure di carattere organizzativo (es. IoT; **sistemi di intelligenza artificiale**; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01	NO	
8. Trattamenti che comportano lo **scambio** tra diversi titolari di dati su **larga scala** con modalità telematiche.	NO	
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri **dati personali raccolti per finalità diverse**	SI	
12. **Trattamenti sistematici di dati genetici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	NO	

Altri casi per cui la DPIA è richiesta	Check	Note
La DPIA deriva da un parere o raccomandazione del DPO.	SI	
La DPIA è richiesta da un codice di condotta, da uno standard, da una best practice.	SI	Linee Guida WP29 WP248 e EDPB 1/2026

La valutazione di impatto rientra in almeno uno dei casi previsti dall'art. 35 GDPR

Ambito di applicazione (oggetto della DPIA)

Questa **valutazione di impatto (DPIA) ai sensi dell'art. 35 GDPR** prende in considerazione l'attività di RICERCA SCIENTIFICA nella sua accezione più ampia, svolta in relazione allo Studio meglio indicato in copertina della presente DPIA.
A tale proposito ed ai fini del presente documento, il termine ""RICERCA"" deve intendersi sinonimo di ""Sperimentazione Clinica"", ""Studio Clinico"", ""Indagine Clinica"", ""Studio"", ""Progetto di Ricerca"" (o ""Protocollo di Ricerca"" o ""Protocollo"").
La tipologia di Studio oggetto della presente DPIA è meglio indicata a seguire ed è comunque individuato dal Protocollo.

Contesto specifico

L’art. 35 GDPR prevede lo svolgimento di una valutazione di impatto quando un tipo di trattamento, allorché prevede in particolare l’uso di nuove tecnologie, considerati la natura, l’oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35.1 GDPR).
In particolare, una valutazione di impatto è richiesta nel caso di trattamento di categorie particolari di dati su larga scala (art. 35.3.b GDPR), nonché negli altri casi previsti dal Garante per la protezione dei dati personali con provvedimento n. 467 del 11/10/2018 [doc. web n. 9058979], tra cui ad es. il caso dei trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo), oppure dei trattamenti di categorie particolari di dati ai sensi dell’art. 9 GDPR interconnessi con altri dati personali raccolti per finalità diverse.
In una politica di protezione dei dati personali approcciata al rischio, con riferimento alla conduzione di detta attività, l’Ente ha ritenuto opportuno procedere in modo granulare, combinado ed addizionando nel loro complesso le valutazioni derivanti dalle **DPIA**:
- **del Centro Promotore**, che descrive l'attività di Ricerca come da Protocollo e valuta primariamente i rischi connaturati al Protocollo stesso;
- **propria generale quale Centro Sperimentale**, che l'Ente ha già adottato a valere quale valutazione di impatto unica (trasversale o generale), avente ad oggetto trattamenti simili che presentino rischi analoghi, la quale descrive le attività proprie e dunque trasversali di tutti gli Studio e ne valuta i rischi intrinsecamente connessi;
- **propria specifica o integrativa, a valere quale "addendum"** alla DPIA del Promotore ed alla propria DPIA generale, ove viene descritta l'attività di trattamento dello Studio in particolare, anche con riferimento e richiamo a quanto descritto nel Protocollo, nonché vengono analizzati i rischi specifici oggetto delle operazioni di trattamento in cui si sostanzia lo Studio.
La possibilità di procedere in tal modo è ammessa dall’ultima parte del par. 1 dell’art. 35 GDPR secondo cui “Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.”
Anche il considerando 92 GDPR dispone che “Vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata”.
Le stesse “Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento ‘possa presentare un rischio elevato’ ai sensi del regolamento 2016/679"", adottate dal c.d. Gruppo (Working Party) 29 (istituzione europea consultiva poi sostituita dallo European Data Protection Board - EDPB, ossia il Comitato Europeo per la Protezione dei Dati) il 4 aprile 2017 nella versione successivamente emendata e adottata il 4 ottobre 2017, stabiliscono che “È possibile utilizzare un’unica DPIA per valutare più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. In effetti, le valutazioni di impatto mirano a svolgere un’analisi sistematica di situazioni nuove che potrebbero comportare rischi elevati per i diritti e le libertà delle persone fisiche, e non occorre condurre una DPIA per quei trattamenti - svolti in un contesto specifico e per una specifica finalità – che siano già stati oggetto di analisi."" Dette Linee Guida anzi suggeriscono tale soluzione, in quanto ""[...] in casi del genere, sarebbe opportuno che una DPIA utilizzabile come riferimento venga condivisa o resa accessibile al pubblico, con l’obbligo di dare attuazione alle misure in essa delineate, mentre si dovrebbe giustificare la scelta di condurre una DPIA isolata.”, ciò anche al fine di evitare DPIA singole su operazioni di trattamento comuni o comunque simili che potrebbero condurre a valutazioni disomogenee e potenzialmente contraddittorie.

Pubblicazione DPIA	**SI**
Luogo pubblicazione (sito web etc.)	La DPIA è disponibile nel sito del centro locale di sperimentazione al seguente link: https://trasparenza.aulss3.veneto.it/trasparenza-sperimentazioni

Condivisione esterna DPIA (comunicazione altri soggetti)	**NO**
A chi e per quale motivo	.

1. Descrizione sistematica del trattamento.

	Check	Dettaglio	Note				
Ruolo svolto dall'Ente nello Studio		Centro Sperimentale					
Il Centro Promotore ha svolto una DPIA e dove è disponibile?	SI	La DPIA è disponibile nel sito del Promotore al seguente link: https://www.mango-group.it/studi/recruiting-planned/endometrial					
Il Centro Sperimentale ha svolto una DPIA generale e dove è disponibile?	SI	La DPIA è disponibile nel sito del centro locale di sperimentazione al seguente link: https://trasparenza.aulss3.veneto.it/trasparenza-sperimentazioni					
Tipologia di Studio		Osservazionale	Retrospettivo	No Profit	Multicentrico	---	---
Finalità		L'obiettivo primario dello studio è valutare l'efficacia della combinazione pembrolizumav-lenvatinib in termini di sopravvivenza libera da progressione (PSF), nelle pazienti con cancro endometriale avanzato.					
Dati trattati		DATI PARTICOLARI art. 9 GDPR	DPART: dati relativi alla salute	DPART: dati genetici	DCOM: età	DCOM: sesso	Ogni altro dato necessario alla conduzione dello Studio secondo il Protocollo.
Interessati coinvolti		pazienti	Persone decedute	Persone non contattabili	Persone vive	---	---
Interesse legittimo (se applicabile)	**N/A**						
Periodo di conservazione		10 anni	I dati contenuti nelle fonti di origine seguono il ciclo di vita proprio definito dalla normativa di settore (massimario di scarto).				
Descrizione funzionale del trattamento		Il trattamento di dati personali della singola attività di Ricerca oggetto dello Studio e le singole operazioni che lo costituiscono sono meglio definiti e descritti nel singolo Protocollo di Ricerca che deve intendersi parte integrante della presente DPIA, nonché nella DPIA del Promotore.					
E stato nominato lo Sperimentatore Principale?	SI	Lo Sperimentatore principale nominato è la Dott.ssa Alessandra Baldoni					
Lo Sperimentatore Principale si avvale di un team?	SI	Lo Sperimentatore principale si avvale di un team					
Come vengono reclutati gli interessati?		In sede di visita per le persone vive che prestano il consenso.					
Come vengono raccolti i dati (CRF)?		Tramite CRF					
Come vengono selezionati i dati oggetto dello Studio (fonti)?		Cartelle cliniche dei pazienti					
Come vengono pseudonimizzati i dati?		ID univoco assistito					
Come vengono anonimizzati i dati (se lo sono)?		Non applicabile					
Come e dove vengono conservati i dati?		I dati fonte vengono conservati presso le rispettive Unità dei P.I. I dati vengono inseriti nelle schede raccolta dati del Promotore e quindi inviati al Promotore stesso secondo le specifiche proprie di ciascun Protocollo di Studio.					
Come vengono elaborati i CRF/eCRF?		Secondo il Protocollo di Studio					
Quali risorse vengono utilizzate per lo Studio?		Secondo il Protocollo di Studio					
Come vengono comunicati i dati al Promotore?		Scheda raccolta dati					
I dati sono oggetto di pubblicazione scientifica?	SI	Come da accordo tra Sponsor e Centro Sperimentale.					

Il Comitato Etico si è espresso favorevolmente e con quali eventuali integrazioni?	SI	Il Comitato Etico si è espresso favorevolmente sul Protocollo di Studio e relativa DPIA già predisposta dallo Sponsor.
Codici di condotta (se applicabile)	**NO**	Non vi sono codici di condotta, ma standard applicabili (vedi sotto).

Ambito del trattamento: estensione del trattamento (volume o scala dato il numero degli interessati o dei dati trattati, estensione geografica o organizzativa, frequenza o durata per gli interessati etc.)		L'estensione del trattamento è esposta nel Protocollo e nella DPIA del Promotore.
Contesto del trattamento: circostanze e ambiente (casi d'uso, processi aziendali supportati, stato del titolare del trattamento e rapporto con gli interessati, categorie di interessati e potenziali gruppi vulnerabili, trattamento transfrontaliero, trasferimenti internazionali, ecc.).		Il contesto è esposto nel Protocollo e nella DPIA del Promotore.

Trasferimento transfrontaliero	NO	Non sono previsti trasferimenti internazionali extra UE-SEE.	
Paesi terzi / organizz. internazionali		-	
		-	
		-	
		-	

Tipo di trattamento svolto		Come da Protocollo.
Mezzi del trattamento (asset)		I mezzi del trattamento sono analiticamente esposti nel Protocollo.

Standard applicabili	**SI**	Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 [9069637], D.M. Giustizia 15 marzo 2019, pubblicato nella Gazzetta Ufficiale n. 71 del 25 marzo 2019, nei limiti della loro applicabilità e compatibilità (tenuto conto che a mente dell'art. 2.2 di dette Regole "Le presenti regole deontologiche non si applicano ai trattamenti per scopi statistici e scientifici connessi con attività di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari, ovvero con attività comparabili in termini di significativa ricaduta personalizzata sull'interessato, che restano regolati dalle pertinenti disposizioni.")
		Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati n. 146 del 5 giugno 2019, Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019 (prescrizioni nn. 4 per i dati genetici e 5 per la ricerca scientifica, nei limiti di applicabilità e compatibilità considerato che detta ultima prescrizione riguarda gli studi condotti senza consenso)
		Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice - 9 maggio 2024 [10016146]
		Regolamento UE 536/2014 sui medicinali per uso umano, noto anche come "Regolamento Europeo sulle Sperimentazioni Cliniche"
		Regolamento (UE) 2017/745 sui dispositivi medici (Medical Device Regulation, "MDR")
		Regolamento (UE) 2017/746 sui dispositivi medici in vitro
		Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" 4 aprile 2017 modificate e adottate il 4 ottobre 2017 (WP29 - EDPB WP248/2017)
		Linee Guida Ricerca Scientifica EDPB 01/2026
		Opinion 05/2014 on Anonymisation Techniques Adopted on 10 April 2014
		Decreto del Ministero della Salute del 30 novembre 2021, recante "Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto legislativo 14 maggio 2019, n. 52".
		Determina Pres. 424-2024 (AIFA) Linea Guida in materia di semplificazione regolatoria ed elementi di decentralizzazione ai fini della conduzione di sperimentazioni cliniche dei medicinali in conformità al regolamento (UE) n.536/2014.Determina Pres. 425-2024 (AIFA) Linea Guida per la classificazione e conduzione degli studi osservazionali sui farmaci (in precedenza, Linee Guida AIFA 20 marzo 2008 - GU Serie Generale n.76 del 31 marzo 2008)

		Dichiarazione di Helsinki “Principi etici per la ricerca biomedica che coinvolge gli esseri umani”, adottata nella XVIII Assemblea Generale della World Medical Association tenutasi nel giugno del 1964, e successive modifiche
		Convenzione del Consiglio d'Europa per la protezione dei diritti dell'uomo e della dignità dell'essere umano nei confronti dell'applicazione della biologia e della medicina “Convenzione sui diritti dell'uomo e la biomedicina”, sottoscritta ad Oviedo il 4 aprile 1997 e ratificata con la legge 28 marzo 2001, n. 145
		Decreto Legislativo n. 137 del 5 agosto 2022, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/745 nonché per l'adeguamento alle disposizioni del regolamento (UE) 2020/561, per quanto riguarda le date di applicazione di alcune delle sue disposizioni
		Decreto del Ministero della Sanità del 15 luglio 1997, recante “Recepimento delle linee guida dell'Unione europea di buona pratica clinica per la esecuzione delle sperimentazioni cliniche dei medicinali”

2. Analisi del trattamento.

	Check	Dettaglio	Dettaglio	Dettaglio	Note
Il trattamento è lecito (basi giuridiche) corretto e trasparente (art. 5.1.a GDPR)	IMPLEMENTATO	Il trattamento avviene sulla base delle condizioni di legittimità ed ulteriori condizioni di liceità previste rispettivamente dagli articoli 6 e 9 GDPR e/o art. 110 o art. 110-bis Codice Privacy, come di seguito esplicato.			

Studi con consenso	SI		
Art. 6 GDPR	Art. 6.1.a) GDPR: l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;		Il consenso viene raccolto previa resa di apposita informativa, secondo le modalità previste dal Protocollo.
Art. 9 GDPR	Art. 9.2.a) GDPR: l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di trattamento delle categorie particolari di dati personali;		

Studi senza consenso (anche parziale) per fini di ricerca medica, biomedica ed epidemiologica	SI		
	Art. 6.1.e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;		
	Art. 9.2.j) GDPR: il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, par. 1 GDPR, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.		
	art. 110 (seconda parte) Codice Privacy: Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice (Si applicano le garanzie disposte dal Garante con Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice del 9 maggio 2024 doc. web n. 10016146, per cui i titolari del trattamento di dati sulla salute per finalità di ricerca medica, biomedica e epidemiologica riferiti a soggetti deceduti o non contattabili devono altresì svolgere e pubblicare la valutazione di impatto, ai sensi dell'art. 35 GDPR, dandone comunicazione al Garante).		
	N/A	Sono invocati: 1. motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione. Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione dello studio la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento).	
	SI	Sono invocati: 2. motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti (ad esempio, nei casi in cui lo studio riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute). Con riferimento a tali motivi di impossibilità organizzativa, le seguenti prescrizioni concernono anche il trattamento dei dati di coloro i quali, all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente) risultino essere al momento dell'arruolamento nello studio: - deceduti o - non contattabili. Resta fermo l'obbligo di rendere l'informativa agli interessati inclusi nella ricerca in tutti i casi in cui, nel corso dello studio, ciò sia possibile e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dal Regolamento.	

	N/A	Sono invocati: 3. motivi di salute riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso. In tali casi, lo studio deve essere volto al miglioramento dello stesso stato clinico in cui versa l'interessato. Inoltre, occorre comprovare che le finalità dello studio non possano essere conseguite mediante il trattamento di dati riferiti a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso o con altre metodologie di ricerca. Ciò, avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché all'attendibilità dei risultati conseguibili in relazione alle specifiche finalità dello studio. Con riferimento a tali motivi, deve essere acquisito il consenso delle persone indicate nell´art. 82, comma 2, lett. a), del Codice come modificato dal d.lgs. n. 101/2018. Ciò, fermo restando che sia resa all'interessato l'informativa sul trattamento dei dati non appena le condizioni di salute glielo consentano, anche al fine dell'esercizio dei diritti previsti dal Regolamento.	
In applicazione delle disposizioni previste dal Garante per l'applicazione dell'art. 110 Codice Privacy, come si è tentato di contattare le persone coinvolte dallo Studio e quali sono i motivi che viceversa hanno reso impossibile tale contatto?		Il P.I svolge i tentativi previsti (solitamente 3) e nei casi di impossibilità al contatto redige l'apposita dichiarazione sostitutiva del consenso. I tentativi sono costituiti da: 1) verifica dell'esistenza in vita tramite anagrafe regionale / aziendale; 2) impiego dei recapiti telefonici in possesso nel centro; 3) l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente.	
In applicazione dell'art. 110 Codice Privacy, la presente DPIA viene pubblicata e dove?	**SI**	La Dpia integrativa è disponibile nel sito web aziendale al seguente link: https://trasparenza.aulss3.veneto.it/Sperimentazioni	

Studi senza consenso per fini di ricerca scientifica che prevedono il trattamento ulteriore di dati personali, compresi quelli particolari, laddove lo Studio è promosso da un Istituto di Ricovero e Cura a Carattere Scientifico (IRCCS) che invoca l'art. 110-bis Codice Privacy	**N/A**	Nel Protocollo e nell'informativa il Promotore non invoca l'art. 110-bis Codice Privacy, cosicché la norma si ritiene non applicabile nel caso di specie.	
	Art. 6.1.e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;		
	Art. 9.2.j) GDPR: il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, par. 1 GDPR, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.		
	art. 110-bis comma 4 Codice Privacy (IRCCS): 4. Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 GDPR.		
	art. 110 (prima parte) Codice Privacy: 1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.		
	FAQ Garante IRCCS: Nel caso di Studio promosso da un IRCCS si applica l'art. 110-bis comma 4 Codice Privacy nonché le FAQ predisposte dal Garante in materia. Come da FAQ n. 2 del Garante a proposito di ricerca scientifica condotta dagli IRCCS, gli IRCCS possono fondare il trattamento dei dati personali raccolti per scopi di cura per ulteriori finalità di ricerca in campo medico, biomedico e epidemiologico sull'art. 110-bis, comma 4 del Codice, in base al quale "Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento". L'art. 110-bis, comma 4 del Codice costituisce una di quelle disposizioni di legge, che si inseriscono nello spazio di normazione lasciato agli Stati membri, ai sensi dell'art. 9, par. 2, lett. j) del Regolamento, alle quali fa riferimento l'art. 110 (primo comma, primo periodo) del Codice nella parte in cui prevede che: "1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, [...] ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento". Come da FAQ n. 2 del Garante a proposito di ricerca scientifica condotta dagli IRCCS, l'art. 110-bis, comma 4 del Codice non definisce quali sono le tipologie di ricerche mediche alle quali esso si applica, limitandosi a indicare l'ambito di applicazione oggettivo della norma che riguarda appunto gli studi promossi dagli IRCCS. La disposizione trova pertanto applicazione in relazione ad ogni tipo di ricerca medica, biomedica, epidemiologica, prospettica e retrospettiva, promossa da tali Istituti ivi inclusi gli studi multicentrici, sia svolti nell'ambito delle reti di ricerca degli IRCCS che in quelli multicentrici promossi da tali istituti con la partecipazione di enti che non godono di tale riconoscimento.		

	La DPIA è comunque pubblicata.				

Studi che perseguono finalità di interesse pubblico e sanità pubblica	**NO**				
	Art. 6.1.e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;				
	Art. 9.2.g) GDPR: il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;				
	art. 2-sexies Codice Privacy				
Indicare la base normativa	-				
	N/A	u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;			
	N/A	v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;			
	N/A	cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);			
Indicazione della base normativa in forza della quale è condotta la Ricerca	-				

Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità sanitarie (art. 8 legge 132/2025)	**NO**				
	Art. 6.1.e) GDPR: il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;				
	Art. 9.2.g) GDPR: il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;				
	art. 8 legge 132/2025: i trattamenti in oggetto, svolti da soggetti pubblici e privati senza scopo di lucro, dagli IRCCS, nonché da soggetti privati operanti nel settore sanitario nell'ambito di progetti di ricerca a cui partecipano soggetti pubblici e privati senza scopo di lucro o IRCCS, sono dichiarati di rilevante interesse pubblico in attuazione degli articoli 32 e 33 della Costituzione e nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, lettera g), del GDPR. Ai medesimi fini, fermo restando l'obbligo di informativa in favore dell'interessato, che può essere assolto anche mediante un'informativa generale messa a disposizione nel sito web del titolare del trattamento e senza ulteriore consenso dell'interessato ove inizialmente previsto dalla legge, è sempre autorizzato l'uso secondario di dati personali privi degli elementi identificativi diretti, anche appartenenti alle categorie indicate all'articolo 9 GDPR, da parte dei soggetti predetti, salvi i casi nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute. Negli ambiti in oggetto o per le finalità di cui all'articolo 2-sexies, comma 2, lettera v), del Codice Privacy (finalità di governo) è sempre consentito, previa informativa all'interessato ai sensi dell'articolo 13 GDPR, il trattamento per finalità di anonimizzazione, pseudonimizzazione o sintetizzazione dei dati personali, anche appartenenti alle categorie particolari di cui all'articolo 9 GDPR. I trattamenti di dati in oggetto devono essere comunicati al Garante per la protezione dei dati personali con l'indicazione di tutte le informazioni previste dagli articoli 24, 25, 32 e 35 GDPR, nonché con l'indicazione espressa, ove presenti, dei soggetti responsabili del trattamento (art. 28 GDPR), e possono essere avviati decorsi trenta giorni dalla predetta comunicazione se non sono stati oggetto di provvedimento di blocco disposto dal Garante per la protezione dei dati personali. Restano fermi i poteri ispettivi, interdittivi e sanzionatori del Garante per la protezione dei dati personali.				

Le finalità sono limitate, determinate, esplicite e legittime (art. 5.1.b GDPR)	**IMPLEMENTATO**	Le finalità di ogni trattamento sono specificamente indicate dal Protocollo e meglio esplicitate nell'informativa.			

I dati personali sono adeguati, pertinenti e limitati (minimizzazione) (art. 5.1.c. GDPR)	**IMPLEMENTATO**	In base al principio di minimizzazione dei dati, vengono raccolti (o conferiti) i soli dati strettamente necessari per il raggiungimento della finalità perseguita per il singolo caso di specie.	Sono adottate tecniche di pseudonimizzazione / anonimizzazione necessarie alla conduzione dello Studio, secondo quanto previsto dal Protocollo.	L'Ente si riserva di invocare il principio di anonimizzazione relativa elaborato dalla Corte di Giustizia nella sentenza "Deloitte" (sentenza C-413/23 P del 4 settembre 2025).	

I dati sono esatti (qualità dei dati) (art. 5.1.d GDPR)	**IMPLEMENTATO**	I dati sono verificati nella loro esattezza prima del loro trattamento nell'ambito delle attività di Ricerca, secondo i criteri di verifica meglio illustrati nel Protocollo e comunque secondo i migliori standard applicabili alle attività di Ricerca e specificamente a quelle oggetto del Protocollo. Nel caso di modifica dei dati, essi sono prontamente aggiornati e nel caso integrati.

La conservazione è limitata (art. 5.1.e GDPR)	**IMPLEMENTATO**	Il periodo di conservazione dei dati di origine dipende dal singolo rapporto nell'ambito del quale avviene il trattamento. Ad esempio Il tempo conservazione dei dati contenuti nella cartella clinica, utilizzati nell'ambito dello studio, è illimitato. I dati dei pazienti acquisiti con altri sistemi (ad es. questionari etc.) sono conservati fino alla definizione della pubblicazione degli esiti della ricerca, ovvero secondo la definizione delle tempistiche valutate durante la stesura del progetto e in accordo alla normativa vigente. I tempi di conservazione dei risultati e degli altri esiti della Ricerca è indicato nel Protocollo. I dati contenuti nelle fonti, di cui sopra, seguono il ciclo di vita proprio definito dalla normativa di settore (massimario di scarto). Ogni altro diverso termine di legge compatibilmente con il Protocollo.

I dati sono trattati in modo sicuro (integrità e riservatezza) (art. 5.1.f GDPR)	**IMPLEMENTATO**	I dati sono trattati con procedure rigorose al fine di mantenerli integri, secondo le regole di trattamento previste dal Protocollo. Il trattamento avviene sotto la direzione dello Sperimentatore Principale (P.I.) individuato per lo Studio e sono materialmente svolti da professionisti tenuti al segreto professionale. La comunicazione dei dati tra Centro Sperimentale e Promotore avviene in modo da mantenere i dati integri e riservati, adottando le migliori tecniche di pseudonimizzazione o anonimizzazione secondo lo stato dell'arte ed in particolare quelle previste dal Protocollo.

Il titolare è in grado di dimostrare il rispetto dei principi (accountability) (art. 5.2 GDPR)	**IMPLEMENTATO**	Il titolare adotta un sistema privacy che prevede la dimostrabilità documentale dell'accountability, mediante un Regolamento, nomine, informative ed ogni altro adempimento richiesto dalla disciplina vigente, come meglio illustrato nell'elenco delle misure di mitigazione del rischio. In particolare, il P.I. ed il proprio team sono espressamente designati ai sensi dell'art 29 GDPR e art. 2-quaterdecies Codice Privacy, l'informativa è inserita nel fascicolo del Progetto oggetto di approvazione da parte del Comitato Etico, gli eventuali responsabili sono nominati con apposito contratto ai sensi dell'art. 28 GDPR. Laddove sia raccolto il consenso, tale raccolta avviene in forma libera, informata, gratuita ed espressa. Negli altri casi, il titolare documenta i motivi per cui il consenso non è raccoglibile, al fine di invocare la base giuridica prevista dall'art. 110 Codice Privacy.

Le informazioni sono fornite all'interessato (art. 12, 13 e 14 GDPR)?	**IMPLEMENTATO**	Gli Interessati sono informati mediante informative rese ai sensi dell'art. 13 GDPR nel caso di raccolta presso l'Interessato o ai sensi dell'art. 14 GDPR nel caso di trattamento di dati NON raccolti presso l'Interessato. Per i rapporti che prevedono la presenza fisica dell'Interessato le informative sono rese mediante apposita modulistica, anche cartacea, rimessa nelle mani dirette dell'Interessato o debitamente pubblicata e consultabile dall'Interessato. Per i rapporti che non prevedono la presenza fisica dell'Interessato, le informative sono pubblicate online e comunque rese consultabili all'Interessato.	
È garantito il diritto di accesso (art. 15 GDPR)?	**IMPLEMENTATO**	Il diritto può essere esercitato mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.	
È garantito il il diritto di rettifica e/o integrazione (art. 16 GDPR)?	**IMPLEMENTATO**	Il diritto può essere esercitato mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.	
È garantito il diritto di cancellazione (art. 17 GDPR)?	**IMPLEMENTATO**	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto, mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.	
		Gli interessati hanno il diritto di ottenere la cancellazione dei propri dati personali, ma il GDPR prevede delle eccezioni a questo diritto. Esiste un'eccezione specifica per le situazioni in cui il trattamento è necessario per scopi di ricerca scientifica. Questa eccezione si applica solo se il diritto alla cancellazione rischia di rendere impossibile o di pregiudicare gravemente l'obiettivo di condurre la ricerca scientifica e se il titolare del trattamento ha adottato garanzie adeguate (vedi sezione 6.2.2 Linee Guida EDPB RIcerca Scientifica).	

È garantito il diritto di limitazione (art. 18 GDPR)?	**IMPLEMENTATO**	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto, mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.	
È garantito il il diritto di portabilità (art. 20 GDPR)?	**SI**	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto, mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.	
È garantito il diritto di opposizione (art. 21 GDPR)?	**IMPLEMENTATO**	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto (in particolare, se lo Studio è condotto con il consenso dell'interessato), mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.	
		Gli interessati hanno il diritto di opporsi al trattamento dei loro dati personali, ma ci sono limitazioni a questo diritto quando i dati personali sono trattati per scopi di ricerca scientifica. I titolari del trattamento possono rifiutare un'opposizione, se il trattamento è necessario per l'esecuzione di un compito svolto per motivi di interesse pubblico ai sensi del diritto dell'Unione o dello Stato membro. Questo include casi in cui un interesse legittimo perseguito dal titolare del trattamento o da una terza parte coincide con un interesse pubblico (vedi sezione 6.3 Linee Guida EDPB Ricerca Scientifica).	

È garantito il diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona (art. 22 GDPR)?	**IMPLEMENTATO**	Il diritto è garantito di default.	Nel caso di applicazione di sistemi di Intelligenza Artificiale (AI), si osserveranno rigorosamente la disciplina europea dettata dal Regolamento (UE) 2024/1689 (AI ACT) e la disciplina nazionale prevista dal D.Lgs. 132/2025, con particolare riferimento alle previsioni degli articoli 7 e seguenti, tra cui in primo luogo i principi della sorveglianza umana e della non discriminazione algoritmica.	Nel caso di ricerca e sperimentazione nella realizzazione di sistemi di AI in ambito sanitario si osserva la disposizione dell'art. 8 Legge 132/2025.	

È garantito il diritto di raccogliere il consenso e di revocarlo (art. 7 GDPR)	**SI**	Il diritto può essere esercitato nei casi previsti dalla disposizione in oggetto, mediante richiesta specifica ai recapiti indicati nelle informative. L'Ente rende riscontro entro un mese ai sensi dell'art. 12 GDPR, salvo proroga comunicata ai sensi e nei casi previsti dalla medesima disposizione.Il diritto di revoca del consenso non è applicabile per i trattamenti che si fondano sull'art 110 codice privacy

È garantito il diritto di reclamo (art. 77 GDPR)?	**IMPLEMENTATO**	Il diritto a proporre reclamo all'autorità di controllo o di rivolgersi in alternativa all'autorità giudiziaria (art. 77 GDPR) è garantito come previsto dall'informativa.

Destinatari	**IMPLEMENTATO**	Promotore	Comitato Etico/Autorità regolatorie	Sperimentatore Principale	
		Eventuali responsabili del trattamento/ Altri, se e come da Protocollo.			
		La comunicazione e il trasferimento dei dati per i trattamenti connessi alla presente valutazione d'impatto può avvenire previa sottoscrizione di un accordo specifico e comunque, in coerenza con quanto previsto dalla normativa vigente e pattuito nel protocollo di Ricerca.			

Sono osservate le regole previste per il trattamento dei dati personali da parte dei responsabili per conto del titolare (art. 28 GDPR)?	**N/A**	Il trattamento non prevede la nomina di responsabili del trattamento da parte del titolare

Sono osservate le garanzie riguardanti trattamenti internazionali (capo V GDPR)?	**N/A**	Non sono previsti trasferimenti internazionali extra UE-SEE.	-	-	-

È garantita la privacy by design (art. 25.1 GDPR)	**IMPLEMENTATO**	Il principio è garantito dal Protocollo
È garantita la privacy by default (art. 25.2 GDPR)	**IMPLEMENTATO**	Il principio è garantito dal Protocollo

Sono previste misure di sicurezza (art. 32 GDPR)	**IMPLEMENTATO**	Sono applicate le misure di sicurezza trasversali elencate nel foglio 4.4 Misure di sicurezza.	Sono applicate le ulteriori misure di sicurezza specifiche previste dal Protocollo.		

3. Necessità e proporzionalità del trattamento.

	Check	Dettaglio	Note
Il trattamento è necessario?	SI	La necessità del trattamento è illustrata dal Protocollo.	
Il trattamento è proporzionale?	SI	La proporzionalità del trattamento è illustrata dal Protocollo.	

Minacce al trattamento

Una minaccia è un evento o una circostanza che può concretizzarsi e incidere negativamente sui diritti e sulle libertà degli interessati.
Nel contesto di un trattamento di dati personali per la ricerca scientifica, le minacce principali, anche in un sistema ben progettato, sono di natura strutturale e derivano dalla potenziale violazione dei principi di riservatezza, integrità o disponibilità.

Tipo di Minaccia	Descrizione
Re-identificazione (Collegamento)	Nonostante l'uso di pseudonimizzazione, si verifica un evento (anche fortuito o dovuto a un attacco esterno) che permette di collegare i dati pseudonimi o aggregati a un interessato specifico, violando il principio di Riservatezza.
Rivelazione Indesiderata (Disclosure)	La diffusione o l'accesso ai dati personali, inclusi i dati sulla salute, a soggetti non autorizzati (es. un ricercatore esterno, un dipendente senza autorizzazione, o il pubblico) in violazione del principio di Riservatezza.
Inesattezza o Alterazione dei Dati	L'integrità dei dati viene compromessa, rendendoli inaccurati o modificati, con potenziali conseguenze sui risultati della ricerca e sulle decisioni che ne derivano. Minaccia al principio di Integrità e Esattezza.
Perdita di Disponibilità	I dati non sono accessibili o vengono distrutti (ad esempio, un guasto hardware, un errore di sistema, un attacco ransomware) pregiudicando la possibilità di completare la ricerca. Minaccia al principio di Disponibilità e Conservazione.
Uso Incompatibile (Finalità)	I dati raccolti per una specifica ricerca vengono riutilizzati per scopi successivi che non sono compatibili con la finalità originaria e per i quali non è stata fornita una base giuridica adeguata (es. fini commerciali). Minaccia al principio di Limitazione della Finalità.

Fonte di Rischio	Spiegazione
Natura Sensibile dei Dati	Il trattamento riguarda dati relativi alla salute (Art. 9 GDPR), che sono intrinsecamente ad alto rischio e richiedono garanzie specifiche.
Uso di Identificatori Univoci (Pseudonimizzazione)	La scelta di pseudonimizzare i dati (invece di anonimizzarli) mantiene il potenziale di re-identificazione, poiché la chiave di collegamento è ancora esistente (anche se conservata separatamente).
Lungo Periodo di Conservazione	La necessità per la ricerca scientifica di conservare i dati per periodi molto lunghi (Art. 5, par. 1, lett. e, GDPR) aumenta la "finestra di esposizione" a possibili minacce (es. attacchi informatici, errori umani, obsolescenza tecnologica).
Set di Dati Ricchi e Complessi	L'uso di big data o la combinazione di set di dati diversi (es. dati genetici, clinici, ambientali) aumenta il rischio di re-identificazione tramite la correlazione incrociata delle informazioni.
Trasferimenti Internazionali	La condivisione dei dati con partner di ricerca in Paesi extra-UE espone i dati a regimi normativi diversi, creando una potenziale debolezza legale/organizzativa.
Mancanza di Trasparenza Progettuale	Una informazione (Art. 13/14 GDPR) troppo generica non permette all'interessato di comprendere appieno i rischi futuri sul riutilizzo dei dati.

Potenziale Impatto	Esempio di Danno per l'Interessato
Discriminazione	La divulgazione di dati sulla salute (es. una patologia genetica o cronica) può portare al rifiuto di un impiego o di una copertura assicurativa.
Danno alla Reputazione/Stigma Sociale	La re-identificazione e la divulgazione di risultati di ricerca personali (es. l'associazione a particolari stili di vita o condizioni mediche) causano imbarazzo, isolamento o perdita di dignità.
Perdita del Controllo sui Dati	A causa di un uso incompatibile, l'interessato perde la capacità di esercitare i propri diritti (es. opposizione, rettifica) su dati che sono stati ormai distribuiti o utilizzati per un fine non previsto.
Danno Finanziario/Frode	Se i dati sanitari sono associati ad altri identificatori, la loro divulgazione può facilitare il furto d'identità o frodi mediche.
Incertezza/Angoscia	La consapevolezza di una violazione dei dati (data breach) o la diffusione di risultati di ricerca errati (dovuti a inesattezza) può causare stress psicologico.

In sintesi, i rischi più alti in questo contesto (ricerca scientifica/medica) sono quasi sempre legati alla potenziale re-identificazione e divulgazione di dati sulla salute, data la loro natura altamente sensibile e le conseguenze personali che ne derivano. La DPIA, pertanto, dimostra che le misure adottate (pseudonimizzazione, cifratura, segregazione dei dati, accordi contrattuali rigorosi, formazione del personale) riducono il rischio di questi specifici impatti a un livello accettabile.

4.1 Analisi rischio inerente.

#ID	Descrizione Minaccia	Fonte Minaccia	Conseguenze	Considerata	Probabilità Originaria	Impatto Originario	Rischio Inerente (Originario)	Media Rischio Inerente
1	Incendio	Ambientale	ID	N/A	2	4	8,000	15,000
2	Allagamento	Ambientale	ID		2	3	6,000	
3	Crollo o altro fattore naturale/fisico	Ambientale	ID		2	3	6,000	
4	Furto di archivi o di singoli dati	Umana	RID		3	5	15,000	
5	Accesso non autorizzato	Umana	RI		3	5	15,000	
6	Comunicazione non autorizzata	Umana	R		3	5	15,000	
7	Diffusione non autorizzata	Umana	R		3	5	15,000	
8	Modifica dati non autorizzata	Umana	RID		3	5	15,000	
9	Distruzione dati non autorizzata	Umana	ID		3	5	15,000	
10	Perdita dati o dispositivo contenente dati	Umana	RID		3	4	12,000	
11	Diffusione credenziali accesso	Umana	R		3	5	15,000	
12	Vittima di phishing o altra manipolazione	Umana	RID		3	5	15,000	
13	Altro trattamento illecito doloso	Umana	RID		3	5	15,000	
14	Altro trattamento illecito colposo	Umana	RID		3	5	15,000	
15	Mancata soddisfazione dei diritti	Umana	RID		2	5	10,000	
16	Cessazione rapporto / turnover	Umana	RID		2	3	6,000	
17	Attacco informatico	Tecnica	RID		3	5	15,000	
18	Virus informatico	Tecnica	RID		3	5	15,000	
19	Intromissione nel sistema	Tecnica	RID		3	5	15,000	
20	Danno tecnico informatico	Tecnica	RID		2	5	10,000	
21	Malfunzionamento informatico	Tecnica	RID		2	5	10,000	
22	Malfunzionamento tecnico	Tecnica	RID		2	4	8,000	
23	Altri fattori di divulgazione dati	Tecnica	R		3	5	15,000	
24	Altri fattori di corruzione dati	Tecnica	I		3	5	15,000	
25	Altri fattori di indisponibilità dei dati	Tecnica	D		3	5	15,000	
26	Mancata consapevolezza privacy	Organizzativa	RID		3	4	12,000	
27	Inosservanza principi/adempimenti privacy	Organizzativa	RID		3	4	12,000	
28	Carenza di personale/Turnover elevato	Organizzativa	RID		2	3	6,000	
29	Altre inefficienze organizzative	Organizzativa	RID		3	3	9,000	

RISCHIO INERENTE (ORIGINARIO)	ALTO

Nella presente scheda sono illustrate le possibili minacce, la loro natura/fonte (Ambientale, Umana, Tecnica, Organizzativa), le possibili conseguenze sui dati personali in termini di Perdita di Riservatezza (R), Perdita di Integrità (I), Perdita di Disponibilità (D), eventualmente anche combinate tra di loro. Il grado di rischio è considerato primariamente nella sua natura inerente, cioè originaria prima dell'applicazione delle misure di mitigazione, ed è calcolato come prodotto di fattori tra la probabilità che quell'evento minaccioso si verifichi e le conseguenze che esso possa arrecare ai diritti ed alle libertà delle persone fisiche coinvolte in relazione alla possibile perdita "RID".

Conseguenze	
R	Perdita di Riservatezza
I	Perdita di Integrità
D	Perdita di Disponibilità
RID	Perdita di Riservatezza + Integrità + Disponibilità
RI	Perdita di Riservatezza + Integrità
RD	Perdita di Riservatezza + Disponibilità
ID	Perdita di Integrità + Disponibilità

Natura/Fonte Minaccia	
Ambientale	La minacca deriva da fattori ambientali o naturali, quali il fuoco o l'acqua, i quali possono coinvolgere gli archivi, analogici o elettronici.
Umana	La minaccia deriva da fattori umani (comportamenti umani) siano essi dolosi o colposi.
Tecnica	La minaccia deriva da aspetti tecnici, quali malfunzionamenti, accidentali o causati da atti intenzionali.
Organizzativa	La minaccia deriva da fattori organizzativi, ad esempio da mancanza di personale, da mancata formazione, da mancanza di istruzioni etc.

4.2 Protocolli.

#ID	PROTOCOLLI	RISCHIO INERENTE (ORIGINARIO)	PROTOCOLLO	MISURA	MISURA	MISURA	MISURA	MISURA	MISURA	MISURA	MISURA	NOTE	VALUTAZIONE	VALORE
	LIVELLO DEL PROTOCOLLO DA CONSIDERARE IN BASE AL RISCHIO INERENTE	**ALTO**												
A	**Politica di sicurezza e procedure per la protezione dei dati personali**													
A.1	L'organizzazione documenta la propria politica di trattamento dei dati personali	**Basso**	**SI**	Manuale/Regolamento Sistema Privacy	Misure di tracciabilità (log etc.)	Politica di gestione degli accessi	Contratto di responsabile art. 28 GDPR	Nomina Autorizzato art. 29 GDPR	Informative				**4**	
A.2	La politica di sicurezza è revisionata su base annuale	**Basso**	**SI**	Nomina DPO	Test periodici sulle misure di sicurezza (penetration test, vulnerability assessment etc.)								**4**	
A.3	Esiste una politica di sicurezza dedicata e separata per quanto riguarda il trattamento dei dati personali, approvata dalla direzione e comunicata a tutta l'organizzazione interna ed esterna	**Medio**	**SI**	Manuale/Regolamento Sistema Privacy	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2								**4,5**	
A.4	Esistono ruoli e responsabilità del personale, misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, responsabili del trattamento o ad altri soggetti terzi coinvolti nel trattamento dei dati personali	**Medio**	**SI**	Manuale/Regolamento Sistema Privacy	Nomina (contratto) Responsabile art. 28 GDPR	Nomina Autorizzato art. 29 GDPR	Nomina Referente Privacy	Nomina Responsabile/Referente IT					**4,5**	**4,417**
A.5	Esiste ed è mantenuto un inventario di politiche/procedure specifiche relative alla sicurezza dei dati personali, sulla base della politica di sicurezza generale	**Medio**	**SI**	Manuale/Regolamento Sistema Privacy	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2								**4,5**	
A.6	La politica di sicurezza è revisionata su base semestrale	**Alto**	**SI**	Nomina DPO	Audit periodici	Test periodici sulle misure di sicurezza (penetration test, vulnerability assessment etc.)							**5**	

B	**Ruoli e responsabilità**

B.1	Sono definiti e assegnati ruoli e responsabilità relativi al trattamento dei dati personali in conformità alla politica di sicurezza	Basso	SI	Manuale/Regolamento Sistema Privacy	Formazione di una lista degli incaricati autorizzati per classi omogenne di incarico	Formazione di una lista degli incaricati autorizzati su base individuale	Referente Privacy interno	Responsabile/Referente IT	Istruzioni al Personale	Misure per l'archiviazione digitale	Misure per l'archiviazione cartacea		4	4,500
B.2	Sono predisposte misure per la revoca dei diritti e delle responsabilità per l'accesso degli operatori al sistema informativo, con le rispettive procedure, per il caso di assenza temporanea o definitiva dell'operatore	Basso	SI	Nomina amministratore sistema	Nomina Autorizzato art. 29 GDPR								4	
B.3	Sono nominate le persone incaricate ai compiti di sicurezza specifici, compresa quella di un responsabile della sicurezza	Medio	SI	Nomina amministratore sistema	Nomina Autorizzato art. 29 GDPR	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2							4,5	
B.4	Risulta nomina formale documentata del responsabile della sicurezza e definizione documentata dei suoi compiti e responsabilità	Alto	SI	Nomina amministratore sistema	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2								5	
B.5	Esiste separazione dei compiti e delle responsabilità nelle aree di possibile conflitto, in modo da ridurre le opportunità di modifica non autorizzata, non intenzionale o l'uso improprio dei dati personali	Alto	SI	Nomina Autorizzato art. 29 GDPR	Nomina Autorizzato art. 29 GDPR	Manuale/Regolamento Sistema Privacy							5	
C	**Politica di controllo degli accessi**													
C.1	Sono previste procedure di controllo di accesso (log etc.), nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)	Basso	SI	Misure di tracciabilità (log etc.)	Controllo degli accessi logici								4	

C.2	Sono previste misure di sicurezza per la concessione dei diritti di accesso degli operatori al sistema informativo e restrizioni per ruoli utente specifici	**Medio**	**SI**	Manuale/Regolamento Sistema Privacy	29	Policy di consultazione dei dati genetici trattati con strumenti elettronici previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note ai soggetti all'uopo designati e di dispositivi, anche biometrici, in loro possesso							**4,5**	**4,500**
C.3	Sono previste eventuali misure di sicurezza per la segregazione dei ruoli di controllo degli accessi (ad es. richiesta di accesso, autorizzazione all'accesso, amministrazione dell'accesso)	**Medio**	**SI**	Nomina amministratore sistema	Nomina Autorizzato art. 29 GDPR	Policy di consultazione dei dati genetici trattati con strumenti elettronici previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note ai soggetti all'uopo designati e di dispositivi, anche biometrici, in loro possesso							**4,5**	
C.4	Sono definiti e assegnati a membri del personale specifici e limitati ruoli con diritti di accesso di sistema	**Alto**	**SI**	Nomina Autorizzato art. 29 GDPR									**5**	

D	**Gestione delle risorse**													
D.1	Esiste un inventario dell'infrastruttura hardware (server, pc etc.), software (gestionali, applicativi, etc.) e di rete. L'inventario dovrebbe includere almeno le seguenti informazioni: risorsa informatica, tipo (es. server, postazione di lavoro), ubicazione (fisica o elettronica)	**Basso**	**SI**	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2	Inventario tecnico-informatico								**4**	

D.2	Le risorse IT sono oggetto di revisione e aggiornamento regolare	**Basso**	**SI**	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2									**4**	**4,375**
D.3	Sono previste eventuali misure di sicurezza e procedure per la definizione dei ruoli di accesso alle varie componenti dell'infrastruttura	**Medio**	**SI**	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2									**4,5**	
D.4	Le risorse IT sono oggetto di revisione e aggiornamento su base annuale	**Alto**	**SI**	Audit periodici	Test periodici sulle misure di sicurezza (penetration test, vulnerability assessment etc.)	Misure NIS2: si rinvia alla separata documentazione							**5**	
E	**Cambio di gestione**													
E.1	Sono previste procedure applicate per le modifiche al sistema IT: regole di registrazione e monitoraggio delle modifiche	**Basso**	**SI**	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2									**4**	**4,500**
E.2	Sono previste eventuali procedure per lo sviluppo di software, se applicabile	**Basso**	**N/A**											
E.3	Sono previste eventuali regole per il cambio dell'operatore o per la sua definitiva cessazione: comunicazione ai mittenti della posta elettronica e simili	**Alto**	**SI**	Manuale/Regolamento Sistema Privacy	Disciplinare uso Strumenti IT								**5**	
F	**Responsabili del trattamento**													
F.1	Sono definite e documentate linee guida e procedure formali, concordate tra il titolare e il responsabile del trattamento prima dell'inizio delle attività, che devono obbligatoriamente seguire lo stesso livello di sicurezza dei dati personali	**Basso**	**SI**	Manuale/Regolamento Sistema Privacy	Nomina (contratto) Responsabile art. 28 GDPR	Audit periodici							**4**	**4,000**
F.2	Sono previste tempistiche di informazione al titolare da parte del responsabile del trattamento in merito a una violazione dei dati personali	**Basso**	**SI**	Procedura Data Breach									**4**	
F.3	Si provvede a formale accordo tra il titolare e il responsabile del trattamento su requisiti e obblighi formali, previa fornitura documentale sufficiente di conformità da parte del responsabile del trattamento	**Basso**	**SI**	Nomina (contratto) Responsabile art. 28 GDPR									**4**	
F.4	È prevista regolare verifica della conformità del responsabile del trattamento (audit del responsabile del trattamento)	**Medio**	**PARZIALMENTE**	Audit periodici									**3**	
F.5	Sono previsti specifici accordi di riservatezza/non divulgazione ai dipendenti del responsabile del trattamento incaricati di elaborare dati	**Alto**	**SI**	Nomina (contratto) Responsabile art. 28 GDPR									**5**	

G	Gestione degli incidenti / violazione dei dati pesonali													
G.1	Esiste un piano tecnico di disaster recovery e di risposta agli incidenti di sicurezza / violazioni, con relative procedure	Basso	SI	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2									4	4,375
G.2	Sono previste procedure tecniche di alert per gli incidenti, le violazioni, le quasi-violazioni (near miss)	Basso	SI	Procedura Data Breach	Misure NIS2: si rinvia alla separata documentazione								4	
G.3	Esiste ed è documentato un piano di risposta agli incidenti, comprese possibili azioni di mitigazione e una chiara assegnazione dei ruoli	Medio	SI	Procedura Data Breach	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2	Manuale/Regolamento Sistema Privacy							4,5	
G.4	Esiste un sistema di registrazione degli incidenti e delle violazioni dei dati personali insieme ai dettagli relativi all'evento e alle azioni di mitigazione eseguite	Alto	SI	Procedura Data Breach									5	

H	Business continuity													
H.1	Sono previste misure di sicurezza per garantire il livello richiesto di continuità e disponibilità del sistema IT in caso di incidente/violazione dei dati	Basso	SI	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2	Procedure di back-up e ripristino	Procedure di back-up e ripristino							4	4,600
H.2	É previsto un piano tecnico di business continuity, con evidenza delle azioni ed assegnazione dei ruoli nel caso di evento pregiudizievole	Medio	SI	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2									4,5	
H.3	Sono previste eventuali misure per l'individuazione del livello di qualità dei servizi principali ed essenziali garantiti in caso di incidente/violazione dei dati	Medio	SI	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2	Procedure di resilienza dei sistemi di trattamento dopo un data breach								4,5	
H.4	É prevista la nomina di personale specifico con responsabilità, autorità e competenze necessarie per gestire la coninuità operativa in caso di incidente/violazione dei dati personali	Alto	SI	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2	Nomina Referente CSIRT								5	
H.5	È presente una struttura alternativa a seconda dell'organizzazione e del tempo di inattività accettabile del sistema IT	Alto	SI	Procedure di resilienza dei sistemi di trattamento dopo un data breach	Procedure di back-up e ripristino								5	

I	**Riservatezza del personale**													
I.1	Sono previste misure di comunicazione dei ruoli, delle responsabilità e degli obblighi relativi al trattamento dei dati personali, durante il processo di preassunzione e/o inserimento lavorativo	**Basso**	**SI**	Manuale/Regolamento Sistema Privacy	Nomina Autorizzato art. 29 GDPR	Formazione del Personale	Istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere	Individuazione delle soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute	Individuazione di cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti	Policy per garantire il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati	Individuazione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente e notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso		**4**	**4,500**
I.2	Esiste un impegno dei dipendenti al rispetto della politica di sicurezza dell'organizzazione e firma dei rispettivi accordi di riservatezza e non divulgazione, prima di assumere le proprie funzioni	**Medio**	**SI**	Nomina Autorizzato art. 29 GDPR	Sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale	Determinazione di un ordine di prenotazione e chiamata degli interessati prescindendo dalla loro individuazione nominativa							**4,5**	
I.3	Esiste un vincolo a specifiche clausole di riservatezza di dipendenti coinvolti nel trattamento ad alto rischio dei dati personali	**Alto**	**SI**	Nomina Autorizzato art. 29 GDPR	Policy di consultazione dei dati genetici trattati con strumenti elettronici previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note ai soggetti all'uopo designati e di dispositivi, anche biometrici, in loro possesso	Individuazione di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute							**5**	
J	**Formazione**													

J.1	Sono previste regole tecniche di informazione ai dipendenti dei controlli di sicurezza del sistema IT che riguardano il loro lavoro quotidiano, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)	Basso	SI	Misure di tracciabilità (log etc.)	Controllo degli accessi logici	Disciplinare uso Strumenti IT							4	4,500
J.2	Sono previsti eventuali programmi di formazione del personale	Medio	SI	Formazione del Personale									4,5	
J.3	É previsto un piano di formazione con scopi e obiettivi definiti su base annua	Alto	SI	Formazione del Personale									5	
K	**Controllo accessi e autenticazione**													
K.1	Esisten un sistema di controllo degli accessi, che preveda la creazione, l'approvazione, la revisione e l'eliminazione degli account utente, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)	Basso	SI	Disciplinare uso Strumenti IT									4	4,375
K.2	Sono previste misure di sicurezza per l'eventuale uso di account utente comuni; regole applicative per la gestione da parte degli operatori che vi accedono	Basso	SI	Disciplinare uso Strumenti IT									4	
K.3	Sono previste procedure di autenticazione per l'accesso al sistema IT: utente/password o altre forme di autenticazione	Basso	SI	Credenziali di Autenticazione (User + Password)									4	
K.4	Sono previste misure di sicurezza per impedire l'uso di password non complesse	Basso	SI	Credenziali di Autenticazione (User + Password)									4	
K.5	Sono previste eventuali regole di composizione della password: lunghezza della password, complessità, periodo di validità e numero di tentativi di accesso non riusciti accettabili	Medio	SI	Procedura per l'affidamento delle credenziali agli incaricati	Disciplinare uso Strumenti IT								4,5	
K.6	Si provvede alla custodia delle password	Medio	SI	Procedura per l'affidamento delle credenziali agli incaricati									4,5	
K.7	É prevista l'autenticazione a due fattori	Medio	SI	Verifica doppio passaggio (two-step verification - verifica a due fattori)									5	
K.8	Sono previste forme di autenticazione del dispositivo in rete	Alto	SI	Controllo degli accessi logici									5	
L	**Registrazione e monitoraggio**													
L.1	Si provvede all'eventuale registrazione dei file di log, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)	Basso	SI	Misure di tracciabilità (log etc.)									4	4,300
L.2	Sono previste modalità di protezione dei file di registro, contrassegnati con data e ora, da manomissioni e accessi non autorizzati. Criteri di determinazione dell'ora (UTC)	Basso	SI	Controllo degli accessi logici									4	
L.3	Si provvede all'eventuale registrazione degli accessi e degli interventi degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta/cancellazione/modifica dei diritti utente	Medio	SI	Misure di tracciabilità (log etc.)									4,5	

L.4	Sono previste eventuali procedure per l'integrità dei file di log	**Medio**	**SI**	Procedure per assicurare la riservatezza, l'integrità, la disponibilità dei dati (RID)									**4,5**	
L.5	Sono previsti eventuali alert per le manomissioni dei sistemi di registrazione degli accessi	**Medio**	**SI**										**4,5**	
M	**Sicurezza server / database**													
M.1	Sono previste modalità di configurazione dei server; privilegi di accesso	**Basso**	**SI**	Nomina amministratore sistema									**4**	**4,417**
M.2	Sono previsti criteri per la minimizzazione dei dati trattati nei server	**Basso**	**SI**	Procedure per la comunicazione dei dati genetici con sistemi riservati	Cifratura e pseudonimizzazione dei dati genetici contenuti in banche dati								**4**	
M.3	Sono previste eventuali soluzioni di crittografia su file o cartelle specifiche	**Medio**	**SI**	Pseudonimizzazione / Cifratura / Crittografia	Anonimizzazione								**4,5**	
M.4	É prevista l'eventuale crittografia delle unità di archiviazione	**Medio**	**SI**	Pseudonimizzazione / Cifratura / Crittografia	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2								**4,5**	
M.5	Sono previste eventuali tecniche di pseudonimizzazione, laddove applicate	**Medio**	**SI**	Pseudonimizzazione / Cifratura / Crittografia	Anonimizzazione								**4,5**	
M.6	Sono previste tecniche di database che supportano la privacy (es. query autorizzate, crittografia ricerca, ecc.)	**Alto**	**SI**	Pseudonimizzazione / Cifratura / Crittografia									**5**	
N	**Sicurezza della postazione di lavoro**													
N.1	Sono previste misure di sicurezza per impedire agli operatori di disattivare o ignorare le impostazioni di sicurezza	**Basso**	**SI**	Procedura per l'affidamento delle credenziali agli incaricati									**4**	**4,167**
N.2	Esistono sistemi e strumenti antivirus, firewall ed altre misure di sicurezza analoghe	**Basso**	**SI**	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2	Firewall	Antivirus							**4**	
N.3	Sono previste regole per non permettere agli operatori di disporre di privilegi per installare o disattivare applicazioni software non autorizzate	**Basso**	**SI**	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2									**4**	
N.4	Si provvede al timeout di sessione per l'assenza temporanea dell'operatore (screensaver)	**Basso**	**SI**										**4**	
N.5	Si provvede ad aggiornamenti di sicurezza critici	**Basso**	**SI**										**4**	
N.6	É prevista una frequenza nella configurazione di antivirus	**Medio**	**SI**	Antivirus									**4,5**	

N.7	Sono previste eventuali misure tecniche per impedire l'archiviazione di informazioni su dispositivi esterni (es. USB, DVD, dischi rigidi esterni)	Alto	PARZIALMENTE	Manuale/Regolamento Sistema Privacy									3	
N.8	Sono previste eventuali misure per la restrizione dell'accesso ad internet	Alto	SI	Disciplinare uso Strumenti IT									5	
N.9	Si provvede alla crittografia completa sulle unità centrali del sistema operativo	Alto	SI	Pseudonimizzazione / Cifratura / Crittografia									5	
O	**Sicurezza di rete / comunicazione**													
O.1	Sono previste misure di crittografia tramite protocolli TLS/SSL per l'accesso ad Internet	Basso	SI	Protocolli sicurezza web (https, TSL, SSL etc.)									4	3,500
O.2	Sono previste eventuali regole per l'attivazione dell'accesso wireless al sistema IT	Medio	SI										4,5	
O.3	Sono previste eventuali misure per l'accesso remoto al sistema informatico (ad es. VPN per smart working o simili)	Medio	SI										4,5	
O.4	Sono previsti strumenti firewall e sistemi di rilevamento delle intrusioni	Medio	SI	Firewall									4,5	
O.5	Sono previste modalità di blocco della connessione ad internet alle postazioni utilizzate per il trattamento dei dati personali	Alto	NO										1	
O.6	Sono previste misure di segregazione della rete informatica	Alto	SI	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2	Partizionamento								5	
O.7	Si abilita l'accesso al sistema IT mediante tecniche di pre-autorizzazione quali il filtraggio MAC o il Network Access Control (NAC)	Alto	NO										1	
P	**Backup**													
P.1	Sono previste procedure di backup e ripristino	Basso	SI	Procedure di back-up e ripristino	Piano di Disaster Recovery / Business Continuity	Politiche di sicurezza (resilienza sistemi dopo attacco, verifica misure tecniche)	Procedure di resilienza dei sistemi di trattamento dopo un data breach						4	4,333
P.2	Sono previste regole di custodia e di protezione fisica ed ambientale delle strutture e dei supporti di backup	Basso	SI										4	
P.3	Sono previste regole di monitoraggio per la corretta esecuzione dei backup	Basso	SI	Procedure di back-up e ripristino									4	
P.4	Esiste una frequenza nell'esecuzione dei backup	Basso	SI	Procedure di back-up e ripristino									4	
P.5	Sono previsti eventuali test dei supporti di backup per l'utilizzo in caso di emergenza	Medio	SI	Procedure di back-up e ripristino									4,5	
P.6	Esiste una frequenza dei backup incrementali	Medio	SI	Procedure di back-up e ripristino									4,5	
P.7	Sono previste modalità di archiviazione delle copie del backup	Medio	SI	Procedure di back-up e ripristino									4,5	

P.8	Sono previsti eventuali servizi di terze parti per attività di backup	Medio	SI										4,5	
P.9	Sono previste eventuali procedure di crittografia ed archiviazione offline dei backup	Alto	SI	Procedure di back-up e ripristino	Pseudonimizzazione / Cifratura / Crittografia								5	
Q	**Dispositivi mobili portatili**													
Q.1	Sono previste misure di sicurezza per l'accesso dei dispositivi mobili e portatili al sistema IT	Basso	SI	Disciplinare uso Strumenti IT									4	2,944
Q.2	Si provvede all'eventuale pre-registrazione dei dispositivi mobili per l'accesso al sistema IT	Basso	NO										1	
Q.3	Sono previste regole per i livelli di protezione dei dispositivi mobili utilizzati in ambito aziendale	Basso	NO										1	
Q.4	Sono previste modalità di definizione di ruoli e responsabilità specifici per la gestione dei dispositivi mobili e portatili	Medio	SI	Disciplinare uso Strumenti IT	Disciplinare uso strumenti Office (Google/Microsoft)								4,5	
Q.5	Sono previste eventuali misure per la cancellazione da remoto dei dati aziendali su dispositivi mobili	Medio	NO										1	
Q.6	Sono previste eventuali misure per la separazione dell'uso privato da quello aziendale nei dispositivi personali mobili	Medio	SI	Disciplinare uso Strumenti IT	Nomina Autorizzato art. 29 GDPR	Nomina Autorizzato art. 29 GDPR							4,5	
Q.7	Sono previste eventuali misure per il caso di smarrimento/furto dei dispositivi mobili	Medio	SI	Disciplinare uso Strumenti IT									4,5	
Q.8	Si provvede all'eventuale autenticazione a due fattori nei dispositivi mobili	Medio	PARZIALMENTE	Verifica doppio passaggio (two-step verification - verifica a due fattori)									3	
Q.9	Sono previste forme di crittografia dei dati aziendali nei dispositivi mobili	Alto	PARZIALMENTE										3	
R	**Sicurezza del ciclo di vita delle applicazioni**													
R.1	Sono previste misure di aggiornamento delle applicazioni e dei software in generale	Basso	SI	Aggiornamento sistema informatico									4	4,111
R.2	Sono previsti requisiti di sicurezza specifici per le applicazioni ed i software in generale	Basso	SI										4	
R.3	Sono adottate tecnologie e tecniche specifiche per supportare la privacy e la protezione dei dati in analogia ai requisiti di sicurezza	Basso	SI	Politiche di privacy by design / by default									4	
R.4	Sono previsti standard e pratiche di codifica sicura	Basso	SI										4	
R.5	Si provvede a test e strumenti di convalida sull'implementazione dei requisiti di sicurezza iniziali	Basso	PARZIALMENTE										3	
R.6	Sono previsti test di vulnerabilità e di penetrazione delle applicazioni, dei software e dell'infrastruttura IT in generale	Medio	SI	Test periodici sulle misure di sicurezza (penetration test, vulnerability assessment etc.)									4,5	
R.7	Si provvede con una certa frequenza ai test di penetrazione	Medio	SI	Test periodici sulle misure di sicurezza (penetration test, vulnerability assessment etc.)									4,5	

R.8	Sono previste modalità di ottenimento delle informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati	**Medio**	**SI**									**4,5**	
R.9	Sono provvede a test e valutazioni delle patch software prima dell'installazione	**Medio**	**SI**									**4,5**	

S	**Cancellazione / eliminazione dei dati**												
S.1	Sono previste misure per la distruzione dei dati contenuti nei dispositivi e supporti IT destinati allo smaltimento	**Basso**	**SI**	Manuale di Gestione Documentale. Massimario di Scarto.								**4**	**4,500**
S.2	Sono previste modalità di distruzione dei documenti cartacei e dei supporti portatili utilizzati per la memorizzazione dei dati personali	**Basso**	**SI**	Manuale di Gestione Documentale. Massimario di Scarto.								**4**	
S.3	Si provvede alla sovrascrittura dei software su tutti i supporti prima di essere eliminati	**Medio**	**N/A**										
S.4	Sono previste nei contratti di servizi regole di distruzione dei dispositivi / cancellazione dei dati (se vengono usati servizi forniti da terze parti)	**Medio**	**SI**	Nomina (contratto) Responsabile art. 28 GDPR								**4,5**	
S.5	Si provvede alla smagnetizzazione dell'hardware dopo la cancellazione del software (se necessario anche distruzione fisica)	**Alto**	**SI**	Manuale di Gestione Documentale. Massimario di Scarto.								**5**	
S.6	É indicato il luogo di distruzione di supporti o archivi cartacei (qualora si utlizzino fornitore esterni del servizio quali responsabile del trattamento)	**Alto**	**SI**	Manuale di Gestione Documentale. Massimario di Scarto.								**5**	

T	**Sicurezza fisica**												
T.1	Sono previste misure di protezione del perimetro fisico dell'infrastruttura (locali server, regole di accesso, serrature e chiavi etc.)	**Basso**	**SI**	Accesso ai locali ai soli autorizzati	Accesso controllato ai locali di conservazione dei dati genetici	Procedure per l'accesso agli archivi dei dati particolari	Conservazione dati sotto chiave	Procedure di conservazione, utilizzo e trasporto dei campioni biologici mediante modalità volte anche a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità	Individuazione dei locali di conservazione dei dati genetici				**4**	**4,278**
T.2	Sono previste misure di identificazione del personale che accede ai locali	**Medio**	**SI**	Accesso ai locali ai soli autorizzati	Accesso controllato ai locali di conservazione dei dati genetici	Procedure per l'accesso agli archivi dei dati particolari	Videosorveglianza	genet					**4,5**	
T.3	Si provvede al controllo e monitoraggio degli accessi alle zone sicure	**Medio**	**SI**										**4,5**	
T.4	Sono installati sistemi di rilevamento degli intrusi	**Medio**	**SI**	Sistema Antifurto									**4,5**	
T.5	Ove applicabile, esistono barriere fisiche per impedire l'accesso non autorizzato	**Medio**	**SI**										**4,5**	
T.6	Si provvede a revisione periodica delle aree interessate da trattamenti	**Medio**	**PARZIALMENTE**										**3**	

T.7	Sono previste misure di protezione contro incendi (estintori etc.), allagamenti (server ed armadi sopraelevati), disfunzioni elettriche (gruppo di continuità UPS), crolli (per terremoto etc.) e simili	**Medio**	**SI**	Misure Antincendio (estintori etc.)	Misure Antiallagamento	Gruppo di Continuità (UPS)	Manutenzione degli impianti						**4,5**	
T.8	Le aree protette sono limitate rispetto al personale di servizi esterni	**Medio**	**SI**	Accesso controllato ai locali di conservazione dei dati genetici									**4,5**	
T.9	Sono previste misure di protezione degli archivi fisici (armadi, schedari, contenitori, cartelline)	**Medio**	**SI**	Accesso ai locali ai soli autorizzati	Accesso controllato ai locali di conservazione dei dati genetici	Procedure per l'accesso agli archivi dei dati particolari							**4,5**	

VALUTAZIONE MEDIA FINALE APPLICAZIONE PROTOCOLLI	**4,195**

Nella presente scheda sono illustrati i protocolli di sicurezza adottati in relazione al grado di rischio inerente come individuato nella scheda precedente. Per ogni protocollo di sicurezza è indicato se detto protocollo è adottato e, laddove possibile, è altresì indicata la specifica misura di sicurezza (o le misure di sicurezza) con cui quel protocollo di sicurezza viene implementato nella realtà del titolare. I protocolli utilizzati sono stati elaborati sulla base di quelli proposti da ENISA.

4.3 Matrice Protocolli-Minacce.

	#	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	MISURE	Incendio	Allagamento	Crollo o altro fattore naturale/fisico	Furto di archivi o di singoli dati	Accesso non autorizzato	Comunicazione non autorizzata	Diffusione non autorizzata	Modifica dati non autorizzata	Distruzione dati non autorizzata	Perdita dati o dispositivo contenente dati	Diffusione credenziali accesso	Vittima di phishing o altra manipolazione	Altro trattamento illecito doloso	Altro trattamento illecito colposo
#ID	PROTOCOLLI	Ambientale	Ambientale	Ambientale	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana
A	**Politica di sicurezza e procedure per la protezione dei dati personali**														
A.1	L'organizzazione documenta la propria politica di trattamento dei dati personali														
A.2	La politica di sicurezza è revisionata su base annuale														
A.3	Esiste una politica di sicurezza dedicata e separata per quanto riguarda il trattamento dei dati personali, approvata dalla direzione e comunicata a tutta l'organizzazione interna ed esterna														
A.4	Esistono ruoli e responsabilità del personale, misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, responsabili del trattamento o ad altri soggetti terzi coinvolti nel trattamento dei dati personali														
A.5	Esiste ed è mantenuto un inventario di politiche/procedure specifiche relative alla sicurezza dei dati personali, sulla base della politica di sicurezza generale														
A.6	La politica di sicurezza è revisionata su base semestrale														
B	**Ruoli e responsabilità**														
B.1	Sono definiti e assegnati ruoli e responsabilità relativi al trattamento dei dati personali in conformità alla politica di sicurezza					4	4	4	4	4					4
B.2	Sono predisposte misure per la revoca dei diritti e delle responsabilità per l'accesso degli operatori al sistema informativo, con le rispettive procedure, per il caso di assenza temporanea o definitiva dell'operatore					4					4			4	4
B.3	Sono nominate le persone incaricate ai compiti di sicurezza specifici, compresa quella di un responsabile della sicurezza					4,5					4,5	4,5	4,5	4,5	4,5
B.4	Risulta nomina formale documentata del responsabile della sicurezza e definizione documentata dei suoi compiti e responsabilità					5					5	5	5	5	5
B.5	Esiste separazione dei compiti e delle responsabilità nelle aree di possibile conflitto, in modo da ridurre le opportunità di modifica non autorizzata, non intenzionale o l'uso improprio dei dati personali					5	5	5	5	5		5			5
C	**Politica di controllo degli accessi**														
C.1	Sono previste procedure di controllo di accesso (log etc.), nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)				4	4	4	4	4	4		4		4	
C.2	Sono previste misure di sicurezza per la concessione dei diritti di accesso degli operatori al sistema informativo e restrizioni per ruoli utente specifici				4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	
C.3	Sono previste eventuali misure di sicurezza per la segregazione dei ruoli di controllo degli accessi (ad es. richiesta di accesso, autorizzazione all'accesso, amministrazione dell'accesso)				4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	
C.4	Sono definiti e assegnati a membri del personale specifici e limitati ruoli con diritti di accesso di sistema				5	5	5	5	5	5		5		5	
D	**Gestione delle risorse**														
D.1	Esiste un inventario dell'infrastruttura hardware (server, pc etc.), software (gestionali, applicativi, etc.) e di rete. L'inventario dovrebbe includere almeno le seguenti informazioni: risorsa informatica, tipo (es. server, postazione di lavoro), ubicazione (fisica o elettronica)	4	4	4							4				
D.2	Le risorse IT sono oggetto di revisione e aggiornamento regolare	4	4	4							4				
D.3	Sono previste eventuali misure di sicurezza e procedure per la definizione dei ruoli di accesso alle varie componenti dell'infrastruttura	4,5	4,5	4,5							4,5				
D.4	Le risorse IT sono oggetto di revisione e aggiornamento su base annuale	5	5	5							5				

E	**Cambio di gestione**													
E.1	Sono previste procedure applicate per le modifiche al sistema IT: regole di registrazione e monitoraggio delle modifiche							4	4	4			4	4
E.2	Sono previste eventuali procedure per lo sviluppo di software, se applicabile													
E.3	Sono previste eventuali regole per il cambio dell'operatore o per la sua definitiva cessazione: comunicazione ai mittenti della posta elettronica e simili					5	5			5	5		5	
F	**Responsabili del trattamento**													
F.1	Sono definite e documentate linee guida e procedure formali, concordate tra il titolare e il responsabile del trattamento prima dell'inizio delle attività, che devono obbligatoriamente seguire lo stesso livello di sicurezza dei dati personali					4								4
F.2	Sono previste tempistiche di informazione al titolare da parte del responsabile del trattamento in merito a una violazione dei dati personali				4	4	4	4	4	4	4	4	4	4
F.3	Si provvede a formale accordo tra il titolare e il responsabile del trattamento su requisiti e obblighi formali, previa fornitura documentale sufficiente di conformità da parte del responsabile del trattamento					4								4
F.4	È prevista regolare verifica della conformità del responsabile del trattamento (audit del responsabile del trattamento)					3								3
F.5	Sono previsti specifici accordi di riservatezza/non divulgazione ai dipendenti del responsabile del trattamento incaricati di elaborare dati					5								5
G	**Gestione degli incidenti / violazione dei dati pesonali**													
G.1	Esiste un piano tecnico di disaster recovery e di risposta agli incidenti di sicurezza / violazioni, con relative procedure	4	4	4	4	4	4	4	4	4	4	4	4	4
G.2	Sono previste procedure tecniche di alert per gli incidenti, le violazioni, le quasi-violazioni (near miss)	4	4	4	4	4	4	4	4	4	4	4	4	4
G.3	Esiste ed è documentato un piano di risposta agli incidenti, comprese possibili azioni di mitigazione e una chiara assegnazione dei ruoli	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5
G.4	Esiste un sistema di registrazione degli incidenti e delle violazioni dei dati personali insieme ai dettagli relativi all'evento e alle azioni di mitigazione eseguite	5	5	5	5	5	5	5	5	5	5	5	5	5
H	**Business continuity**													
H.1	Sono previste misure di sicurezza per garantire il livello richiesto di continuità e disponibilità del sistema IT in caso di incidente/violazione dei dati	4	4	4	4	4	4	4	4	4	4	4	4	4
H.2	É previsto un piano tecnico di business continuity, con evidenza delle azioni ed assegnazione dei ruoli nel caso di evento pregiudizievole	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5
H.3	Sono previste eventuali misure per l'individuazione del livello di qualità dei servizi principali ed essenziali garantiti in caso di incidente/violazione dei dati	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5
H.4	É prevista la nomina di personale specifico con responsabilità, autorità e competenze necessarie per gestire la coninuità operativa in caso di incidente/violazione dei dati personali	5	5	5	5	5	5	5	5	5	5	5	5	5
H.5	È presente una struttura alternativa a seconda dell'organizzazione e del tempo di inattività accettabile del sistema IT	5	5	5	5						5			5	
I	**Riservatezza del personale**													
I.1	Sono previste misure di comunicazione dei ruoli, delle responsabilità e degli obblighi relativi al trattamento dei dati personali, durante il processo di preassunzione e/o inserimento lavorativo					4	4	4	4	4	4	4	4	4
I.2	Esiste un impegno dei dipendenti al rispetto della politica di sicurezza dell'organizzazione e firma dei rispettivi accordi di riservatezza e non divulgazione, prima di assumere le proprie funzioni					4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5
I.3	Esiste un vincolo a specifiche clausole di riservatezza di dipendenti coinvolti nel trattamento ad alto rischio dei dati personali					5		5				5		5
J	**Formazione**													

J.1	Sono previste regole tecniche di informazione ai dipendenti dei controlli di sicurezza del sistema IT che riguardano il loro lavoro quotidiano, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)											4	4		
J.2	Sono previsti eventuali programmi di formazione del personale					4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5
J.3	É previsto un piano di formazione con scopi e obiettivi definiti su base annua					5	5	5	5	5	5	5	5		5
K	**Controllo accessi e autenticazione**														
K.1	Esisten un sistema di controllo degli accessi, che preveda la creazione, l'approvazione, la revisione e l'eliminazione degli account utente, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)					4					4				
K.2	Sono previste misure di sicurezza per l'eventuale uso di account utente comuni; regole applicative per la gestione da parte degli operatori che vi accedono					4	4					4			
K.3	Sono previste procedure di autenticazione per l'accesso al sistema IT: utente/password o altre forme di autenticazione				4	4								4	
K.4	Sono previste misure di sicurezza per impedire l'uso di password non complesse				4	4								4	
K.5	Sono previste eventuali regole di composizione della password: lunghezza della password, complessità, periodo di validità e numero di tentativi di accesso non riusciti accettabili				4,5	4,5								4,5	
K.6	Si provvede alla custodia delle password				4,5	4,5	4,5					4,5		4,5	
K.7	É prevista l'autenticazione a due fattori				5	5								4	
K.8	Sono previste forme di autenticazione del dispositivo in rete				5	5								5	
L	**Registrazione e monitoraggio**														
L.1	Si provvede all'eventuale registrazione dei file di log, nel rispetto del divieto di controllo a distanza dei lavoratori laddove applicabile (art. 4 Statuto dei Lavoratori Legge 300/1970)				4	4	4	4	4	4				4	
L.2	Sono previste modalità di protezione dei file di registro, contrassegnati con data e ora, da manomissioni e accessi non autorizzati. Criteri di determinazione dell'ora (UTC)					4			4	4				4	
L.3	Si provvede all'eventuale registrazione degli accessi e degli interventi degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta/cancellazione/modifica dei diritti utente					4,5			4,5	4,5				4,5	
L.4	Sono previste eventuali procedure per l'integrità dei file di log					4,5			4,5	4,5				4,5	
L.5	Sono previsti eventuali alert per le manomissioni dei sistemi di registrazione degli accessi					4,5			4,5	4,5		4,5		4,5	
M	**Sicurezza server / database**														
M.1	Sono previste modalità di configurazione dei server; privilegi di accesso					4			4	4				4	
M.2	Sono previsti criteri per la minimizzazione dei dati trattati nei server														
M.3	Sono previste eventuali soluzioni di crittografia su file o cartelle specifiche				4,5	4,5	4,5	4,5				4,5	4,5	4,5	4,5
M.4	É prevista l'eventuale crittografia delle unità di archiviazione				4,5	4,5	4,5	4,5				4,5	4,5	4,5	4,5
M.5	Sono previste eventuali tecniche di pseudonimizzazione, laddove applicate				4,5	4,5	4,5	4,5				4,5	4,5	4,5	4,5
M.6	Sono previste tecniche di database che supportano la privacy (es. query autorizzate, crittografia ricerca, ecc.)				5	5	5	5				5	5	5	5
N	**Sicurezza della postazione di lavoro**														
N.1	Sono previste misure di sicurezza per impedire agli operatori di disattivare o ignorare le impostazioni di sicurezza				4	4	4	4	4	4				4	4
N.2	Esistono sistemi e strumenti antivirus, firewall ed altre misure di sicurezza analoghe				4	4							4	4	
N.3	Sono previste regole per non permettere agli operatori di disporre di privilegi per installare o disattivare applicazioni software non autorizzate												4	4	
N.4	Si provvede al timeout di sessione per l'assenza temporanea dell'operatore (screensaver)				4	4					4	4		4	
N.5	Si provvede ad aggiornamenti di sicurezza critici				4	4								4	

N.6	É prevista una frequenza nella configurazione di antivirus				4,5										
N.7	Sono previste eventuali misure tecniche per impedire l'archiviazione di informazioni su dispositivi esterni (es. USB, DVD, dischi rigidi esterni)				3	3	3	3						3	
N.8	Sono previste eventuali misure per la restrizione dell'accesso ad internet												5	5	5
N.9	Si provvede alla crittografia completa sulle unità centrali del sistema operativo				5	5	5	5			5	5	5	5	5
O	**Sicurezza di rete / comunicazione**														
O.1	Sono previste misure di crittografia tramite protocolli TLS/SSL per l'accesso ad Internet												4	4	4
O.2	Sono previste eventuali regole per l'attivazione dell'accesso wireless al sistema IT				4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5	4,5
O.3	Sono previste eventuali misure per l'accesso remoto al sistema informatico (ad es. VPN per smart working o simili)				4,5	4,5	4,5	4,5						4,5	4,5
O.4	Sono previsti strumenti firewall e sistemi di rilevamento delle intrusioni				4,5	4,5	4,5	4,5						4,5	4,5
O.5	Sono previste modalità di blocco della connessione ad internet alle postazioni utilizzate per il trattamento dei dati personali				1	1	1	1			1	1	1	1	1
O.6	Sono previste misure di segregazione della rete informatica				5	5	5	5			5	5	5	5	5
O.7	Si abilita l'accesso al sistema IT mediante tecniche di pre-autorizzazione quali il filtraggio MAC o il Network Access Control (NAC)				1	1								1	
P	**Backup**														
P.1	Sono previste procedure di backup e ripristino	4	4	4	4					4	4		4	4	4
P.2	Sono previste regole di custodia e di protezione fisica ed ambientale delle strutture e dei supporti di backup	4	4	4	4					4	4		4	4	4
P.3	Sono previste regole di monitoraggio per la corretta esecuzione dei backup	4	4	4	4					4	4		4	4	4
P.4	Esiste una frequenza nell'esecuzione dei backup	4	4	4	4					4	4		4	4	4
P.5	Sono previsti eventuali test dei supporti di backup per l'utilizzo in caso di emergenza	4,5	4,5	4,5	4,5					4,5	4,5		4,5	4,5	4,5
P.6	Esiste una frequenza dei backup incrementali	4,5	4,5	4,5	4,5					4,5	4,5		4,5	4,5	4,5
P.7	Sono previste modalità di archiviazione delle copie del backup	4,5	4,5	4,5	4,5					4,5	4,5		4,5	4,5	4,5
P.8	Sono previsti eventuali servizi di terze parti per attività di backup	4,5	4,5	4,5	4,5					4,5	4,5		5	5	5
P.9	Sono previste eventuali procedure di crittografia ed archiviazione offline dei backup	5	5	5	5					5	5		5	5	5
Q	**Dispositivi mobili portatili**														
Q.1	Sono previste misure di sicurezza per l'accesso dei dispositivi mobili e portatili al sistema IT				4	4	4	4	4	4	4	4		4	4
Q.2	Si provvede all'eventuale pre-registrazione dei dispositivi mobili per l'accesso al sistema IT				1	1	1	1	1	1	1	1		1	1
Q.3	Sono previste regole per i livelli di protezione dei dispositivi mobili utilizzati in ambito aziendale					1	1	1				1	1	1	1
Q.4	Sono previste modalità di definizione di ruoli e responsabilità specifici per la gestione dei dispositivi mobili e portatili					4,5	4,5	4,5				4,5	4,5	4,5	4,5
Q.5	Sono previste eventuali misure per la cancellazione da remoto dei dati aziendali su dispositivi mobili												1		
Q.6	Sono previste eventuali misure per la separazione dell'uso privato da quello aziendale nei dispositivi personali mobili												4,5		
Q.7	Sono previste eventuali misure per il caso di smarrimento/furto dei dispositivi mobili				4,5	4,5					4,5	4,5		4,5	
Q.8	Si provvede all'eventuale autenticazione a due fattori nei dispositivi mobili				3	3	3	3	3	3	3	3		3	
Q.9	Sono previste forme di crittografia dei dati aziendali nei dispositivi mobili				3	3	3	3	3	3	3	3		3	
R	**Sicurezza del ciclo di vita delle applicazioni**														
R.1	Sono previste misure di aggiornamento delle applicazioni e dei software in generale				4							4	4	4	
R.2	Sono previsti requisiti di sicurezza specifici per le applicazioni ed i software in generale				4							4	4	4	

R.3	Sono adottate tecnologie e tecniche specifiche per supportare la privacy e la protezione dei dati in analogia ai requisiti di sicurezza				4	4	4	4	4	4	4	4	4	4	4
R.4	Sono previsti standard e pratiche di codifica sicura				4			4			4	4	4	4	
R.5	Si provvede a test e strumenti di convalida sull'implementazione dei requisiti di sicurezza iniziali				3						3	3		3	
R.6	Sono previsti test di vulnerabilità e di penetrazione delle applicazioni, dei software e dell'infrastruttura IT in generale					4,5	4,5	4,5	4,5	4,5				4,5	
R.7	Si provvede con una certa frequenza ai test di penetrazione					4,5	4,5	4,5	4,5	4,5				4,5	
R.8	Sono previste modalità di ottenimento delle informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati					4,5	4,5	4,5	4,5	4,5				4,5	
R.9	Sono provvede a test e valutazioni delle patch software prima dell'installazione					4,5	4,5	4,5	4,5	4,5				4,5	
S	**Cancellazione / eliminazione dei dati**														
S.1	Sono previste misure per la distruzione dei dati contenuti nei dispositivi e supporti IT destinati allo smaltimento					4	4	4		4					
S.2	Sono previste modalità di distruzione dei documenti cartacei e dei supporti portatili utilizzati per la memorizzazione dei dati personali					4	4	4		4					
S.3	Si provvede alla sovrascrittura dei software su tutti i supporti prima di essere eliminati														
S.4	Sono previste nei contratti di servizi regole di distruzione dei dispositivi / cancellazione dei dati (se vengono usati servizi forniti da terze parti)					4,5				4,5	4,5	4,5			
S.5	Si provvede alla smagnetizzazione dell'hardware dopo la cancellazione del software (se necessario anche distruzione fisica)					5				5	5	5			
S.6	É indicato il luogo di distruzione di supporti o archivi cartacei (qualora si utlizzino fornitore esterni del servizio quali responsabile del trattamento)					5				5	5	5			
T	**Sicurezza fisica**														
T.1	Sono previste misure di protezione del perimetro fisico dell'infrastruttura (locali server, regole di accesso, serrature e chiavi etc.)				4	4								4	
T.2	Sono previste misure di identificazione del personale che accede ai locali				4,5	4,5								4,5	
T.3	Si provvede al controllo e monitoraggio degli accessi alle zone sicure				4,5	4,5								4,5	
T.4	Sono installati sistemi di rilevamento degli intrusi				4,5	4,5								4,5	
T.5	Ove applicabile, esistono barriere fisiche per impedire l'accesso non autorizzato				4,5	4,5								4,5	
T.6	Si provvede a revisione periodica delle aree interessate da trattamenti														
T.7	Sono previste misure di protezione contro incendi (estintori etc.), allagamenti (server ed armadi sopraelevati), disfunzioni elettriche (gruppo di continuità UPS), crolli (per terremoto etc.) e simili	4,5	4,5	4,5										4,5	4,5
T.8	Le aree protette sono limitate rispetto al personale di servizi esterni				4,5	4,5								4,5	
T.9	Sono previste misure di protezione degli archivi fisici (armadi, schedari, contenitori, cartelline)				4,5	4,5								4,5	

VALUTAZIONE FINALE MITIGAZIONE PER MINACCIA	**4,413**	**4,413**	**4,413**	**4,148**	**4,195**	**4,135**	**4,128**	**4,203**	**4,255**	**4,216**	**4,190**	**4,196**	**4,163**	**4,221**

Nella presente scheda vengono illustrati in quale modo e misura i protocolli adottati mitigano i rischi inerenti.

15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Mancata soddisfazione dei diritti	Cessazione rapporto / turnover	Attacco informatico	Virus informatico	Intromissione nel sistema	Danno tecnico informatico	Malfunzionamento informatico	Malfunzionamento tecnico	Altri fattori di divulgazione dati	Altri fattori di corruzione dati	Altri fattori di indisponibilità dei dati	Mancata consapevolezza privacy	Inosservanza principi/adempimenti privacy	Carenza di personale/Turnover elevato	Altre inefficienze organizzative
Umana	Umana	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Organizzativa	Organizzativa	Organizzativa	Organizzativa
											4	4	4	4
											4	4	4	4
											4,5	4,5	4,5	4,5
											4,5	4,5	4,5	4,5
											4,5	4,5	4,5	4,5
											5	5	5	5
4	4										4	4	4	4
4	4											4	4	4
		4,5	4,5	4,5	4,5			4,5	4,5	4,5				4,5
		5	5	5	5			5	5	5				5
5	5										5	5	5	5
												4	4	4
	4,5			4,5		4,5		4,5	4,5	4,5		4,5		4,5
	4,5			4,5		4,5		4,5	4,5	4,5		4,5		4,5
	5			5		5		5	5	5		5		5
	4	4	4	4	4	4	4	4	4	4		4		4
	4	4	4	4	4	4	4	4	4	4		4		4
	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5		4,5
	5	5	5	5	5	5	5	5	5	5		5		5

	4	4	4	4	4	4	4	4	4	4		4		4
	5											5	5	5
4											4	4	4	4
4		4	4	4	4	4	4	4	4	4	4	4	4	4
4											4	4	4	4
3		3	3	3	3	3	3	3	3	3	3	3	3	3
5		5	5	5	5	5	5	5	5	5	5	5	5	5
		4	4	4	4	4	4	4	4	4				
		4	4	4	4	4	4	4	4	4				4
		4	4	4	4	4	4	4	4	4				4
		4	4	4	4	4	4	4	4	4				4
		5	5	5	5	5	5	5	5	5				5
		4	4	4	4	4	4	4	4	4		4		4
		4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5		4,5
		4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5
		5	5	5	5	5	5	5	5	5	5	5	5	5
		5	5	5	5	5	5	5	5	5			5	
4	4										4	4	4	4
4,5	4,5										4,5	4,5	4,5	4,5
5								5			5	5	5	5

	4										4	4	4	4
4,5	4,5										4,5	4,5	4,5	4,5
5	5										5	5	5	5
4	4			4						4	4	4	4	4
4	4							4			4	4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4
				4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
				4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
		4	4	4	4	4	4	4	4	4	4	4	4	4
				5				5	5		5	5	5	5
		4	4	4	4			4			4	4	4	4
								4	4			4		4
		4,5	4,5	4,5	4,5			4,5	4,5			4,5		4,5
		4,5	4,5	4,5	4,5			4,5	4,5			4,5		4,5
		4,5	4,5	4,5	4,5			4,5	4,5			4,5		4,5
				4	4			4	4	4		4		4
4				4				4			4	4		4
	4,5	4,5		4,5				4,5				4,5	4,5	4,5
	4,5	4,5		4,5				4,5				4,5	4,5	4,5
	4,5	4,5		4,5				4,5				4,5	4,5	4,5
	5	5		5				5				5	5	5
			4			4	4	4	4	4	4	4		4
			4	4	4	4		4	4	4				4
		4	4	4	4	4	4	4	4	4	4	4		4
				4	4	4	4	4				4	4	4
		4	4	4	4	4	4	4	4	4	4	4	4	4

		4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5				
	3										3	3	3	3
											5	5	5	5
		5	5	5				5				5	5	5
		4		4				4				4	4	4
				4,5				4,5			4,5	4,5	4,5	4,5
	4,5			4,5				4,5			4,5	4,5	4,5	4,5
	4,5			4,5				4,5			4,5	4,5	4,5	4,5
		1	1	1	1	1	1	1	1	1	1	1		1
		5	5	5	5	5	5	5	5	5	5	5		5
				1				1			1			
4	4	4	4	4	4	4	4		4	4	4	4	4	4
4	4	4	4	4	4	4	4		4	4	4	4	4	4
4	4	4	4	4	4	4	4		4	4	4	4	4	4
4	4	4	4	4	4	4	4		4	4	4	4	4	4
4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5	4,5	4,5	4,5
4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5	4,5	4,5	4,5
4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5	4,5	4,5	4,5
5	5	5	5	5	5	5	5		4,5	4,5	4,5	4,5	4,5	4,5
5	5	5	5	5	5	5	5		5	5	5	5	5	5
	4	4	4	4	4	4	4	4			4	4	4	4
	1	1	1	1	1	1	1	1			1	1	1	1
											1	1	1	1
											4,5	4,5	4,5	4,5
	1										1	1	1	1
	4,5										4,5	4,5	4,5	4,5
											4,5	4,5	4,5	4,5
				3				3	3		3	3	3	3
				3				3			3	3	3	3
		4	4	4	4	4		4	4	4				4
		4	4	4	4	4		4	4	4				4

4	4										4	4	4	4
		4	4	4	4	4		4			4	4	4	4
		3	3	3	3	3		3	3	3				
		4,5	4,5	4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
		4,5	4,5	4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
		4,5	4,5	4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
		4,5	4,5	4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
4								4		4	4	4	4	4
4											4	4	4	4
4,5											4,5	4,5	4,5	4,5
5											5	5	5	5
5											5	5	5	5
					4		4				4	4	4	4
				4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
				4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
				4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
	4,5			4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5
					4,5	4,5	4,5			4,5				
					4,5	4,5	4,5	4,5			4,5	4,5	4,5	4,5
	4,5							4,5			4,5	4,5	4,5	4,5

4,323	**4,214**	**4,214**	**4,179**	**4,188**	**4,144**	**4,135**	**4,125**	**4,176**	**4,262**	**4,259**	**4,091**	**4,201**	**4,217**	**4,209**

4.4 Misure di sicurezza.

	MISURE DI SICUREZZA PER TUTTI I TRATTAMENTI	Natura Misura		Note
1	Accesso ai locali ai soli autorizzati	MISURA FISICA	SI	
2	Misure Antincendio (estintori etc.)	MISURA FISICA	SI	
3	Misure Antiallagamento	MISURA FISICA	SI	
4	Sistema Antifurto	MISURA FISICA	SI	
5	Manutenzione degli impianti	MISURA FISICA	SI	
6	Gruppo di Continuità (UPS)	MISURA FISICA	SI	
7	Conservazione dati sotto chiave	MISURA FISICA	SI	
8	Videosorveglianza	MISURA FISICA	SI	
9	Test periodici sulle misure di sicurezza (penetration test, vulnerability assessment etc.)	MISURA TECNICA	SI	
10	Misure di tracciabilità (log etc.)	MISURA TECNICA	SI	
11	Partizionamento	MISURA TECNICA	SI	
12	Antivirus	MISURA TECNICA	SI	
13	Firewall	MISURA TECNICA	SI	
14	Aggiornamento sistema informatico	MISURA TECNICA	SI	
15	Pseudonimizzazione / Cifratura / Crittografia	MISURA TECNICA	SI	
16	Anonimizzazione	MISURA TECNICA	SI	
17	Piano di Disaster Recovery / Business Continuity	MISURA TECNICA	SI	
18	Procedure di back-up e ripristino	MISURA TECNICA	SI	
19	Credenziali di Autenticazione (User + Password)	MISURA TECNICA	SI	
20	Verifica doppio passaggio (two-step verification - verifica a due fattori)	MISURA TECNICA	SI	
	Procedura per l'affidamento delle credenziali agli incaricati	MISURA TECNICA	SI	
21	Politica di gestione degli accessi	MISURA TECNICA	SI	
22	Controllo degli accessi logici	MISURA TECNICA	SI	
23	Protocolli sicurezza web (https, TSL, SSL etc.)	MISURA TECNICA	SI	
24	Nomina amministratore sistema	MISURA TECNICA	SI	
25	Inventario tecnico-informatico	MISURA TECNICA	SI	
26	Misure NIS2 in base alla classificazione del soggetto (rinvio alle separate politiche NIS2	MISURA TECNICA	SI	
27	Classificazione ACN (AC1 > AC4; QC1 > QC4)	MISURA TECNICA	NO	richiesta ai fornitori per i quali la misura sia prevista
28	ISO 27001	MISURA TECNICA	NO	richiesta ai fornitori per i quali la misura sia prevista
29	ISO 27017	MISURA TECNICA	NO	richiesta ai fornitori per i quali la misura sia prevista
30	ISO 27018	MISURA TECNICA	NO	richiesta ai fornitori per i quali la misura sia prevista
31	Manuale/Regolamento Sistema Privacy	MISURA ORGANIZZATIVA	SI	
32	Nomina Referente Privacy	MISURA ORGANIZZATIVA	SI	
33	Nomina Responsabile/Referente IT	MISURA ORGANIZZATIVA	SI	
34	Nomina Autorizzato art. 29 GDPR	MISURA ORGANIZZATIVA	SI	
35	Nomina (contratto) Responsabile art. 28 GDPR	MISURA ORGANIZZATIVA	SI	
36	Nomina DPO	MISURA ORGANIZZATIVA	SI	
	Nomina Referente CSIRT	MISURA ORGANIZZATIVA	SI	
37	Audit periodici	MISURA ORGANIZZATIVA	SI	
38	Istruzioni al Personale	MISURA ORGANIZZATIVA	SI	
39	Misure per l'archiviazione digitale	MISURA ORGANIZZATIVA	SI	
40	Misure per l'archiviazione cartacea	MISURA ORGANIZZATIVA	SI	
41	Formazione del Personale	MISURA ORGANIZZATIVA	SI	
42	Informative	MISURA ORGANIZZATIVA	SI	
43	Disciplinare uso Strumenti IT	MISURA ORGANIZZATIVA	SI	
44	Procedura Data Breach	MISURA ORGANIZZATIVA	SI	
45	Politiche di sicurezza (resilienza sistemi dopo attacco, verifica misure tecniche)	MISURA ORGANIZZATIVA	SI	
46	Procedure di resilienza dei sistemi di trattamento dopo un data breach	MISURA ORGANIZZATIVA	SI	
47	Procedure per assicurare la riservatezza, l'integrità, la disponibilità dei dati (RID)	MISURA ORGANIZZATIVA	SI	
48	Politiche di privacy by design / by default	MISURA ORGANIZZATIVA	SI	
49	ISO 9001	MISURA ORGANIZZATIVA	NO	richiesta ai fornitori per i quali la misura sia prevista
50	Manuale di Gestione Documentale. Massimario di Scarto.	MISURA ORGANIZZATIVA	SI	

/	SANITÀ: MISURE DI SICUREZZA SPECIFICHE	Natura Misura		Note
51	Accesso controllato ai locali di conservazione dei dati genetici	MISURA FISICA	SI	
52	Procedure di conservazione, utilizzo e trasporto dei campioni biologici mediante modalità volte anche a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità	MISURA FISICA	SI	
53	Procedure per la comunicazione dei dati genetici con sistemi riservati	MISURA FISICA	SI	
54	Individuazione dei locali di conservazione dei dati genetici	MISURA FISICA	SI	
55	Procedure per l'accesso agli archivi dei dati particolari	MISURA FISICA	SI	

56	Istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere	MISURA FISICA	SI	
57	Cifratura e pseudonimizzazione dei dati genetici contenuti in banche dati	MISURA TECNICA	SI	
58	Determinazione di un ordine di prenotazione e chiamata degli interessati prescindendo dalla loro individuazione nominativa	MISURA ORGANIZZATIVA	SI	
59	Individuazione delle soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute	MISURA ORGANIZZATIVA	SI	
60	Individuazione di cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti	MISURA ORGANIZZATIVA	SI	
61	Policy per garantire il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati	MISURA ORGANIZZATIVA	SI	
62	Individuazione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso	MISURA ORGANIZZATIVA	SI	
63	Individuazione di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute	MISURA ORGANIZZATIVA	SI	
64	Sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale	MISURA ORGANIZZATIVA	SI	
65	Policy di consultazione dei dati genetici trattati con strumenti elettronici previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note ai soggetti all'uopo designati e di dispositivi, anche biometrici, in loro possesso	MISURA ORGANIZZATIVA	SI	

Natura Misura
MISURA FISICA
MISURA TECNICA
MISURA ORGANIZZATIVA

In questa scheda vengono illustrate le misure di sicurezza adottate in relazione ai protocolli di sicurezza applicati.

4.5 Analisi rischio residuo.

#ID	Descrizione Minaccia	Fonte Minaccia	Conseguenze	Mitigazione del Rischio	Probabilità residua	Impatto Residuo	Rischio residuo	Rischio Residuo
1	Incendio	Ambientale	ID	SI	1	2	2,000	
2	Allagamento	Ambientale	ID	SI	1	1	1,000	
3	Crollo o altro fattore naturale/fisico	Ambientale	ID	SI	1	1	1,000	
4	Furto di archivi o di singoli dati	Umana	RID	SI	1	3	3,000	
5	Accesso non autorizzato	Umana	RI	SI	1	3	3,000	
6	Comunicazione non autorizzata	Umana	R	SI	1	3	3,000	
7	Diffusione non autorizzata	Umana	R	SI	1	3	3,000	
8	Modifica dati non autorizzata	Umana	RID	SI	1	3	3,000	
9	Distruzione dati non autorizzata	Umana	ID	SI	1	3	3,000	
10	Perdita dati o dispositivo contenente dati	Umana	RID	SI	1	2	2,000	
11	Diffusione credenziali accesso	Umana	R	SI	1	3	3,000	
12	Vittima di phishing o altra manipolazione	Umana	RID	SI	1	3	3,000	
13	Altro trattamento illecito doloso	Umana	RID	SI	1	3	3,000	
14	Altro trattamento illecito colposo	Umana	RID	SI	1	3	3,000	
15	Mancata soddisfazione dei diritti	Umana	RID	SI	1	3	3,000	3,000
16	Cessazione rapporto / turnover	Umana	RID	SI	1	1	1,000	
17	Attacco informatico	Tecnica	RID	SI	1	3	3,000	
18	Virus informatico	Tecnica	RID	SI	1	3	3,000	
19	Intromissione nel sistema	Tecnica	RID	SI	1	3	3,000	
20	Danno tecnico informatico	Tecnica	RID	SI	1	3	3,000	
21	Malfunzionamento informatico	Tecnica	RID	SI	1	3	3,000	
22	Malfunzionamento tecnico	Tecnica	RID	SI	1	2	2,000	
23	Altri fattori di divulgazione dati	Tecnica	R	SI	1	3	3,000	
24	Altri fattori di corruzione dati	Tecnica	I	SI	1	3	3,000	
25	Altri fattori di indisponibilità dei dati	Tecnica	D	SI	1	3	3,000	
26	Mancata consapevolezza privacy	Organizzativa	RID	SI	1	2	2,000	
27	Inosservanza principi/adempimenti privacy	Organizzativa	RID	SI	1	2	2,000	
28	Carenza di personale/Turnover elevato	Organizzativa	RID	SI	1	1	1,000	
29	Altre inefficienze organizzative	Organizzativa	RID	SI	1	1	1,000	

RISCHIO RESIDUO	**BASSO**
RISCHIO ACCETTATO	**BASSO**
MOTIVAZIONE DELL'EVENTUALE RIDUZIONE	

Nella presente scheda è espressa l'analisi del rischio residuo, una volta applicate le misure di mitigazione per effetto dell'implementazione dei protocolli di sicurezza e correlate misure di sicurezza.

Conseguenze	
R	Perdita di Riservatezza
I	Perdita di Integrità
D	Perdita di Disponibilità
RID	Perdita di Riservatezza + Integrità + Disponibilità
RI	Perdita di Riservatezza + Integrità
RD	Perdita di Riservatezza + Disponibilità
ID	Perdita di Integrità + Disponibilità

Natura/Fonte minaccia
Ambientale
Umana
Tecnica
Organizzativa

4.6 Comparazione Rischi.

#ID	Descrizione Minaccia	Fonte Minaccia	Conseguenze	Considerata	Probabilità Originaria	Impatto Originario	Rischio Inerente (Originario)
1	Incendio	Ambientale	ID	N/A	2	4	8,000
2	Allagamento	Ambientale	ID	0	2	3	6,000
3	Crollo o altro fattore naturale/fisico	Ambientale	ID	0	2	3	6,000
4	Furto di archivi o di singoli dati	Umana	RID	0	3	5	15,000
5	Accesso non autorizzato	Umana	RI	0	3	5	15,000
6	Comunicazione non autorizzata	Umana	R	0	3	5	15,000
7	Diffusione non autorizzata	Umana	R	0	3	5	15,000
8	Modifica dati non autorizzata	Umana	RID	0	3	5	15,000
9	Distruzione dati non autorizzata	Umana	ID	0	3	5	15,000
10	Perdita dati o dispositivo contenente dati	Umana	RID	0	3	4	12,000
11	Diffusione credenziali accesso	Umana	R	0	3	5	15,000
12	Vittima di phishing o altra manipolazione	Umana	RID	0	3	5	15,000
13	Altro trattamento illecito doloso	Umana	RID	0	3	5	15,000
14	Altro trattamento illecito colposo	Umana	RID	0	3	5	15,000
15	Mancata soddisfazione dei diritti	Umana	RID	0	2	5	10,000
16	Cessazione rapporto / turnover	Umana	RID	0	2	3	6,000
17	Attacco informatico	Tecnica	RID	0	3	5	15,000
18	Virus informatico	Tecnica	RID	0	3	5	15,000
19	Intromissione nel sistema	Tecnica	RID	0	3	5	15,000
20	Danno tecnico informatico	Tecnica	RID	0	2	5	10,000
21	Malfunzionamento informatico	Tecnica	RID	0	2	5	10,000
22	Malfunzionamento tecnico	Tecnica	RID	0	2	4	8,000
23	Altri fattori di divulgazione dati	Tecnica	R	0	3	5	15,000
24	Altri fattori di corruzione dati	Tecnica	I	0	3	5	15,000
25	Altri fattori di indisponibilità dei dati	Tecnica	D	0	3	5	15,000
26	Mancata consapevolezza privacy	Organizzativa	RID	0	3	4	12,000
27	Inosservanza principi/adempimenti privacy	Organizzativa	RID	0	3	4	12,000
28	Carenza di personale/Turnover elevato	Organizzativa	RID	0	2	3	6,000
29	Altre inefficienze organizzative	Organizzativa	RID	0	3	3	9,000

RISCHIO INERENTE (ORIGINARIO)	**ALTO**

Conseguenze	
R	Perdita di Riservatezza
I	Perdita di Integrità
D	Perdita di Disponibilità
RID	Perdita di Riservatezza + Integrità + Disponibilità
RI	Perdita di Riservatezza + Integrità
RD	Perdita di Riservatezza + Disponibilità
ID	Perdita di Integrità + Disponibilità

Natura/Fonte Minaccia
Ambientale
Umana
Tecnica
Organizzativa

Rischio Inerente		Mitigazione del Rischio	Probabilità residua	Impatto Residuo	Rischio residuo	Rischio Residuo
15,000	in base al valore di Rischio Inerente si valuta l'applicazione dei corrispondenti Protocolli e si applicano le Misure di mitigazione	SI	1	2	2,000	3,000
		SI	1	1	1,000	
		SI	1	1	1,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	2	2,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	1	1,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	2	2,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	3	3,000	
		SI	1	2	2,000	
		SI	1	2	2,000	
		SI	1	1	1,000	
		SI	1	1	1,000	

RISCHIO RESIDUO	BASSO

RISCHIO ACCETTATO	BASSO

4.7 Metriche

PROBABILITA		METRICA DI VALUTAZIONE
Basso	1	La probabilità di accadimento della minaccia è molto bassa, quasi nulla
Basso Medio	2	La probabilità di accadimento della minaccia è bassa, ossia l'accadimento è possibile ma abbastanza remoto
Medio	3	La probabilità di accadimento della minaccia è ordinaria, nei limiti della possibilità, tenuto conto di un grado di valutazione prudente
Medio Alto	4	La probabilità di accadimento della minaccia è medio/alta, per effetto di alcune occasioni di accadimento o di altri elementi analoghi
Alto	5	La probabilità di accadimento della minaccia è molto alta, per effetto di frequenze significative o di altri elementi analoghi

IMPATTO		METRICA DI VALUTAZIONE
Basso	1	L'impatto sui diritti e sulle libertà delle persone è molto basso, quasi nullo
Basso Medio	2	L'impatto sui diritti e sulle libertà delle persone è basso, ma in qualche modo apprezzabile
Medio	3	L'impatto sui diritti e sulle libertà delle persone è medio ed apprezzabile
Medio Alto	4	L'impatto sui diritti e sulle libertà delle persone è rilevante ed incisivo
Alto	5	L'impatto sui diritti e sulle libertà delle persone è grave ed in alcuni casi irreversibile

RISCHIO		METRICA DI VALUTAZIONE
Basso	1-6	Il rischio esiste, ma è basso tenuto, conto dei vari fattori esaminati
Basso Medio	6,0001-7,9999	Il rischio esiste e si avvicina al medio, tenuto conto dei vari fattori esaminati
Medio	8-12	Il rischio è medio ed apprezzabile, tenuto conto dei vari fattori esaminati
Medio Alto	12,0001-14,9999	Il rischio è più alto dell'ordinario, tenuto conto dei vari fattori esaminati
Alto	15-25	Il rischio è molto alto e tende al probabile, tenuto conto dei vari fattori esaminati

METRICA DI VALUTAZIONE RISCHIO PER INDIVIDUARE I PROTOCOLLI DA APPLICARE		
Basso	1-6	BASSO
Basso Medio	6,001-7,999	MEDIO
Medio	8-12	
Medio Alto	12,001-14,999	ALTO
Alto	15-25	

METRICA DI VALUTAZIONE PROTOCOLLO IN BASE AL LIVELLO DI RISCHIO		
SI	RISCHIO BASSO	4
	RISCHIO MEDIO	4,5
	RISCHIO ALTO	5
PARZIALMENTE	RISCHIO BASSO	3
	RISCHIO MEDIO	
	RISCHIO ALTO	
NO	RISCHIO BASSO	1
	RISCHIO MEDIO	
	RISCHIO ALTO	
N/A	RISCHIO BASSO	neutro
	RISCHIO MEDIO	
	RISCHIO ALTO	

METRICA DI VALUTAZIONE PER L'APPLICAZIONE DI PROTOCOLLI E MISURE		
SI	5	la misura risulta pienamente adottata
In modo sufficiente	4	la misura risulta adottata in modo sufficiente
PARZIALMENTE	3	la misura risulta adottata parzialmente o è in corso di adozione
Poco	2	la misura risulta poco adottata
NO	1	la misura non risulta adottata
N/A	neutro	la misura non si applica al caso

GRADO DI MITIGAZIONE PROBABILITÀ E IMPATTO RISPETTO ALL'INERENTE (ORIGINARIO)		
SI	4>5	-2
PARZIALMENTE	3>3,999	-1
NO	1>2,999	0
N/A		neutro

Nella presente scheda sono illustrate le metriche applicate alle valutazioni oggetto della presente DPIA.

5. Coinvolgimento delle parti (DPO e Interessati)

Parti	CHECK	Dettaglio
Il DPO è stato consultato?	SI	Il DPO è stato consultato nel processo di valutazione
Come?		Tramite consultazione diretta e via corrispondenza
Che opinione ha dato?	Il DPO è favorevole a che il trattamento proceda	

Gli interessati o loro rappresentanti sono stati consultati?	NO	
Come?		
Che opinione hanno dato?	-	

Nella presente scheda sono illustrate le consultazioni del DPO, se designato, e degli interessati o dei loro rappresentanti, se del caso.

6. Conclusioni.

Conclusioni del Titolare	CHECK	Dettaglio
A seguito delle valutazioni svolte, il Titolare del trattamento decide di:	Approvare il trattamento.	

Data	22/07/2026
Firma	IL DIRETTORE GENERALE