Valutazione di impatto
Data Protection Impact Assessment
(DPIA)

Ente	**Azienda ULSS 3 Serenissima** Via Don Tosatto 147 30174 Mestre C.F. e P.I. 02798850273

Rappresentante legale	**Direttore Generale**

DPO	**Cervato Law & Business s.r.l. Società tra Avvocati ref. Avv. Piergiovanni Cervato**

Nome del trattamento	**studio retrospettivo multicentrico per la valutazione della SBRT(radioterapia stereotassica corporea) nel ritrattamento di lesioni polmonari inoperabili dopo precedente SBRT(STRILL-IT)**

Centro locale di Sperimentazione	**UOC Radioterapia Ospedale dell'Angelo Mestre**

Rif. art. 35 GDPR
Rif. Guidelines WP29 248/2017
Rif. Provv. Garante n. 467 11/10/2018

19/2/2026

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	il numero di interessati coinvolti non costituisce "larga scala"

Art. 35 par. 4 GDPR - All. 1 provv. Garante n. 467 11/10/2018 [doc. web n. 9058979]	**Check**	**Note**
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)	SI	

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

Descrizione del trattamento	Check	Dettaglio	Dettaglio	Dettaglio	Dettaglio	Dettaglio	Dettaglio	Dettaglio	Dettaglio
Natura		Trattamento misto automatizzato/non automatizzato							
Ambito di applicazione (oggetto)		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		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. A tale proposito, i trattamenti cui si riferisce il presente documento riguardano tutti le attività di **Studio connaturate al medesimo Protocollo**, per cui esse sono comuni e comunque simili a quelle del Centro Promotore e presentano rischi analoghi: quelli del Centro Promotore sono propri e strettamente collegati al Protocollo, quelli del Centro Sperimentale sono propri e comunque connaturati alle specifiche modalità con cui lo Studio è attuato presso il Centro, ovviamente in conformità al medesimo Protocollo. I trattamenti sono quindi considerati, in quest'ottica, comunque simili e presentano tutti rischi da considerarsi analoghi in relazione al contesto, nel senso di omogenei tra di loro, per cui si ritiene possano avvalersi di una valutazione di impatto integrata, combinata tra quella del Promotore (DPIA Promotore), quella generale del Centro Sperimentale (DPIA generale Centro Sperimentale) e quella integrativa oggetto del presente documento (DPIA integrativa o "addendum"). Laddove i rischi fossero viceversa diversi e disomogenei, ad esempio per la particolare tipologia di dati trattati o per la tipologia di interessati coinvolti, l'Ente si riserva di adottare una DPIA specifica.							
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.humanitas.it/ricerca-scientifica/ricerca-osservazionale-retrospettiva/							
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/Sperimentazioni							
Tipologia di Studio		Osservazionale	Retrospettivo	Multicentrico	No Profit	---	---	---	
Finalità		L'obiettivo primario dello studio è valutare la sicurezza, sia nella fase acuta che tardiva del ritrattamento di recidive polmonari trattare dopo SBRT dopo trattamento convenzionale nei pazienti non candidabili a resezione chirurgica							
Dati trattati		DATI PARTICOLARI art. 9 GDPR	DPART: dati relativi alla salute	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**								

Destinatari		Promotore	Comitato Etico/Autorità regolatorie	Sperimentatore Principale	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.	---	---	---	---
Periodo di conservazione		7 anni	I dati contenuti nelle fonti, di cui sopra, 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.							
É stato nominato lo Sperimentatore Principale?	**SI**	Lo sperimentatore principale nominato è Dr.ssa Melissa Scricciolo							
Lo Sperimentatore Principale si avvale di un team ?	**NO**	Lo sperimentatore principale non 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 inserite 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 dati?		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).							

Standard o Linee Guida 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 menti 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)	
		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"	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)	Opinion 05/2014 on Anonymisation Techniques Adopted on 10 April 2014	
Sono stati consultati gli interessati e, se sì, in che modo e quale esito ha dato la consultazione?	**NO**	NO. Ai sensi delle Linee Guida WP248 del WP29 (oggi EDPB) (in particolare pag. 15 del testo italiano), il Titolare ritiene che la consultazione degli interessati o di loro rappresentanti non è opportuna sia per un rischio di pregiudizio alla riservatezza dello Studio, sia perché in ogni caso non prevista dal Protocollo di Ricerca e comunque il suo svolgimento sarebbe sproporzionato e comunque impraticabile a fronte delle modalità operative di svolgimento dello Studio come da Protocollo medesimo.							
É stato consultato il DPO?	**SI**	L'Ente si è consultato con il proprio Responsabile della Protezione dei Dati, il quale ha reso le migliori indicazioni sui criteri di conduzione della presente DPIA, ivi compresi gli standard applicabili e le linee guida, nulla opponendo alla presente DPIA. Il DPO si riserva peraltro di essere specificamente consultato e di poter esprimere il proprio parere ulteriore in relazione alle DPIA specifiche di singoli Studi e/o alle DPIA integrative condotte dal Centro Sperimentale a valere quali addendum di valutazione rispetto alle DPIA svolte dai Centri Promotori (Sponsor).							

Necessità e proporzionalità del trattamento	Check	Dettaglio	Dettaglio	Dettaglio	Dettaglio	Dettaglio	Dettaglio	Dettaglio
Le finalità sono determinate, esplicite e legittime (art. 5, par. 1, lett. b. GDPR)?	SI	La finalità è la conduzione dello Studio avente ad oggetto Ricerca medica, biomedica ed epidemiologica, come Protocollo.						
Il trattamento è lecito in relazione alle specifiche basi giuridiche indicate (art. 5, par. 1, lett. a. GDPR; art. 6 GDPR + art. 9 GDPR + prescrizioni o regole deontologiche in quanto applicabili)?	SI	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 in relazione alle singole tipologie di Studi.						
Studi con consenso	SI	Art. 6.1.a) GDPR: l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;	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;	Il consenso viene raccolto previa resa di apposita informativa, secondo le modalità previste dal Protocollo.				
Studi senza consenso 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).	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	---	---	---
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 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, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività o laddove lo Studio è promosso da un Istituto di Ricerca e Cura a Carattere Scientifico (IRCCS)	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).	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.			
I dati personali sono adeguati, pertinenti e limitati (minimizzazione dei dati) (art. 5, paragrafo 1, lett. c GDPR)?	SI	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 e aggiornati? (art. 5, paragrafo 1, lett. d GDPR)	SI	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, par. 1, lett. e GDPR)?	SI	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.tella clinica						
Il trattamento garantisce integrità e riservatezza? (art. 5, par. 1, lett. f. GDPR)	SI	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 dimostra il rispetto dei principi (accountability) (art. 5 par. 2 GDPR)?	SI	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 e come (art. 12, 13 e 14 GDPR)?	SI	"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 per lo più pubblicate online e rese consultabili all'Interessato mediante apposite pagine web / link / allegati ad e-mail / form contatti, in formato elettronico / digitale."						
È garantito il diritto di accesso e come può essere esercitato (art. 15 GDPR)?	SI	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 e come può essere esercitato (art. 16 GDPR)?	SI	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 e come può essere esercitato (art. 17 GDPR)?	SI	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 limitazione e come può essere esercitato (art. 18 GDPR)?	**SI**	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 portabilità e come può essere esercitato (art. 20 GDPR)?	**SI**	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 opposizione e come può essere esercitato (art. 21 GDPR)?	**SI**	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 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)?	**SI**	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.	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.
È garantito il diritto di revoca del consenso (art. 7 GDPR)?	**SI**	Per gli Studi che si fondano sul consenso è garantito il diritto di revoca del consenso con le stesse modalità con cui è stato raccolto e comunque con le altre modalità previste dall'informativa.	
È garantito il diritto di reclamo (art. 77 GDPR)?	**SI**	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.	
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 al di fuori dell'Unione Europea (capo V GDPR)?	**N/A**	Il trattamento non prevede trasferimenti internazionali	
É attivata la consultazione preventiva del Garante (art. 36 GDPR)?	**N/A**	La consultazine preventiva del Garante non è attivata in quanto non si rientra nei casi di cui all'art. 36 GDPR.	

Esito della valutazione di necessità e proporzionalità	Il trattamento potrebbe ritenersi conforme

#ID	Descrizione Minaccia	Natura Minaccia	Conseguenze	Considerata	Probabilità Originaria	Impatto Originario	Rischio Inerente (Originario)	Media Rischio Inerente
1	Incendio	Ambientale	ID	SI	2	4	8,000	12,931
2	Allagamento	Ambientale	ID	SI	2	3	6,000	
3	Crollo o altro fattore naturale/fisico	Ambientale	ID	SI	2	3	6,000	
4	Furto di archivi o di singoli dati	Umana	RID	SI	3	5	15,000	
5	Accesso non autorizzato	Umana	RI	SI	3	5	15,000	
6	Comunicazione non autorizzata	Umana	R	SI	3	5	15,000	
7	Diffusione non autorizzata	Umana	R	SI	3	5	15,000	
8	Modifica dati non autorizzata	Umana	RID	SI	3	5	15,000	
9	Distruzione dati non autorizzata	Umana	ID	SI	3	5	15,000	
10	Perdita dati o dispositivo contenente dati	Umana	RID	SI	3	4	12,000	
11	Diffusione credenziali accesso	Umana	R	SI	3	5	15,000	
12	Vittima di phishing o altra manipolazione	Umana	RID	SI	4	5	20,000	
13	Altro trattamento illecito doloso	Umana	RID	SI	3	5	15,000	
14	Altro trattamento illecito colposo	Umana	RID	SI	3	5	15,000	
15	Mancata soddisfazione dei diritti	Umana	RID	SI	2	5	10,000	
16	Cessazione rapporto / turnover	Umana	RID	SI	2	3	6,000	
17	Attacco informatico	Tecnica	RID	SI	4	5	20,000	
18	Virus informatico	Tecnica	RID	SI	4	5	20,000	
19	Intromissione nel sistema	Tecnica	RID	SI	4	5	20,000	
20	Danno tecnico informatico	Tecnica	RID	SI	2	5	10,000	
21	Malfunzionamento informatico	Tecnica	RID	SI	2	5	10,000	
22	Malfunzionamento tecnico	Tecnica	RID	SI	2	4	8,000	
23	Altri fattori di divulgazione dati	Tecnica	R	SI	3	5	15,000	
24	Altri fattori di corruzione dati	Tecnica	I	SI	3	5	15,000	
25	Altri fattori di indisponibilità dei dati	Tecnica	D	SI	3	5	15,000	
26	Mancata consapevolezza privacy	Organizzativa	RID	SI	3	4	12,000	
27	Inosservanza principi/adempimenti privacy	Organizzativa	RID	SI	3	4	12,000	
28	Carenza di personale/Turnover elevato	Organizzativa	RID	SI	2	3	6,000	
29	Altre inefficienze organizzative	Organizzativa	RID	SI	3	3	9,000	

RISCHIO INERENTE (ORIGINARIO)	ALTO

Nella presente scheda sono illustrate le possibili minacce, la loro natura (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 minaccia
Ambientale
Umana
Tecnica
Organizzativa

#ID	PROTOCOLLI	RISCHIO INERENTE (ORIGINARIO)	PROTOCOLLO ADOTTATO	MISURA APPLICATA	MISURA APPLICATA	MISURA APPLICATA	MISURA APPLICATA	MISURA APPLICATA	MISURA APPLICATA	MISURA APPLICATA	MISURA APPLICATA	NOTE	VALUTAZIONE	MEDIA
	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**	Regolamento Sistema Privacy	Misure di tracciabilità (log etc.)	Politica di gestione degli accessi	Contratto di responsabile art. 28 GDPR	Lettera di Nomina Autorizzato art. 29 GDPR	Informative / consensi con policy di revisione				**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**	Regolamento Sistema Privacy	Misure NIS2: si rinvia alla separata documentazione								**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**	Regolamento Sistema Privacy	Contratto di responsabile art. 28 GDPR	Lettera di Nomina Autorizzato art. 29 GDPR							**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**	Regolamento Sistema Privacy	Misure NIS2: si rinvia alla separata documentazione								**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**	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	Designazione incaricati autorizzati 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	Designazione Delegati trattamento art. 29 GDPR	Misure NIS2: si rinvia alla separata documentazione							**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: si rinvia alla separata documentazione								**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**	Designazione Delegati trattamento art. 29 GDPR	Designazione incaricati autorizzati art. 29 GDPR	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**	Regolamento Sistema Privacy	Designazione incaricati autorizzati 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**	**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	Designazione incaricati autorizzati 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**	Designazione Delegati trattamento art. 29 GDPR	Designazione incaricati autorizzati 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: si rinvia alla separata documentazione	Inventario tecnico-informatico								**4**	**4,375**
D.2	Le risorse IT sono oggetto di revisione e aggiornamento regolare	**Basso**	**SI**	Misure NIS2: si rinvia alla separata documentazione									**4**	

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: si rinvia alla separata documentazione									**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: si rinvia alla separata documentazione									**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**	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**	Regolamento Sistema Privacy	Contratto di responsabile art. 28 GDPR	Valutazione delle garanzie di compliance privacy di responsabili, sub-responsabili e/o contitolari	Policy di revisione periodica dei rapporti contrattuali con i fornitori						**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**	Contratto di 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	Valutazione delle garanzie di compliance privacy di responsabili, sub-responsabili e/o contitolari	Policy di revisione periodica dei rapporti contrattuali con i fornitori							**3**	
F.5	Sono previsti specifici accordi di riservatezza/non divulgazione ai dipendenti del responsabile del trattamento incaricati di elaborare dati	**Alto**	**SI**	Contratto di 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**	**PARZIALMENTE**	Misure NIS2: si rinvia alla separata documentazione									**3**	
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: si rinvia alla separata documentazione	Regolamento Sistema Privacy							**4,5**	**4,125**
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	Registro 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: si rinvia alla separata documentazione	Back-Up	Definizione delle procedure tecniche di Back-up	Individuazione dell'incaricato al Back-up	Definizione delle procedure organizzative di Back-up					**4**	
H.2	É previsto un piano tecnico di business continuity, con evidenza delle azioni ed assegnazione dei ruoli nel caso di evento pregiudizievole	**Medio**	**PARZIALMENTE**	Misure NIS2: si rinvia alla separata documentazione									**3**	

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**	**PARZIALMENTE**	Misure NIS2: si rinvia alla separata documentazione	Procedure di resilienza dei sistemi di trattamento dopo un data breach								**3**	**4,000**
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: si rinvia alla separata documentazione	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	Definizione delle procedure organizzative di Back-up								**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**	Regolamento Sistema Privacy	Designazione incaricati autorizzati art. 29 GDPR	Formazione del Personale							**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**	Designazione incaricati autorizzati art. 29 GDPR									**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**	Designazione incaricati autorizzati 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	Disciplinare uso strumenti Office (Google/Microsoft)								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	Disciplinare uso strumenti Office (Google/Microsoft)								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)	Procedura per l'affidamento delle credenziali agli incaricati								4	
K.4	Sono previste misure di sicurezza per impedire l'uso di password non complesse	Basso	SI	Procedura per l'affidamento delle credenziali agli incaricati	Procedure di controllo sulle credenziali								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	Disciplinare uso strumenti Google							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**		
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**		**4,300**
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**		

M.2	Sono previsti criteri per la minimizzazione dei dati trattati nei server	Basso	PARZIALMENTE										3	4,250
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: si rinvia alla separata documentazione								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	3,944
N.2	Esistono sistemi e strumenti antivirus, firewall ed altre misure di sicurezza analoghe	Basso	SI	Misure NIS2: si rinvia alla separata documentazione	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	PARZIALMENTE	Misure NIS2: si rinvia alla separata documentazione									3	
N.4	Si provvede al timeout di sessione per l'assenza temporanea dell'operatore (screensaver)	Basso	PARZIALMENTE										3	
N.5	Si provvede ad aggiornamenti di sicurezza critici	Basso	SI										4	
N.6	É prevista una frequenza nella configurazione di antivirus	Medio	SI	Procedura di aggiornamento periodico dell'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										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: si rinvia alla separata documentazione	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**	Back-Up	Definizione delle procedure tecniche di Back-up	Individuazione dell'incaricato al Back-up	Definizione delle procedure organizzative di Back-up	Piano di Disaster Recovery / Business Continuity					**4**	
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**	Definizione delle procedure tecniche di Back-up	Individuazione dell'incaricato al Back-up	Definizione delle procedure organizzative di Back-up							**4**	

P.4	Esiste una frequenza nell'esecuzione dei backup	Basso	SI	Definizione delle procedure organizzative di Back-up									4	4,333
P.5	Sono previsti eventuali test dei supporti di backup per l'utilizzo in caso di emergenza	Medio	SI	Definizione delle procedure organizzative di Back-up									4,5	
P.6	Esiste una frequenza dei backup incrementali	Medio	SI	Definizione delle procedure organizzative di Back-up									4,5	
P.7	Sono previste modalità di archiviazione delle copie del backup	Medio	SI	Definizione delle procedure organizzative di Back-up									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	Definizione delle procedure tecniche di Back-up	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										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	Designazione Delegati trattamento art. 29 GDPR	Designazione incaricati autorizzati 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**	
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**	**PARZIALMENTE**										**3**	
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**	**3,667**
R.7	Si provvede con una certa frequenza ai test di penetrazione	**Medio**	**PARZIALMENTE**	Test periodici sulle misure di sicurezza (penetration test, vulnerability assessment etc.)									**3**	
R.8	Sono previste modalità di ottenimento delle informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati	**Medio**	**PARZIALMENTE**										**3**	
R.9	Si 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 specifico									**4**	**3,417**
S.2	Sono previste modalità di distruzione dei documenti cartacei e dei supporti portatili utilizzati per la memorizzazione dei dati personali	**Basso**	**NO**										**1**	
S.3	Si provvede alla sovrascrittura dei software su tutti i supporti prima di essere eliminati	**Medio**	**NO**										**1**	
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**	Contratto di 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 specifico									**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 specifico									**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						**4**
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						**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**	**NO**										**1**	**4,056**
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	**4,034**

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.

		#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
		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	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
#ID	**PROTOCOLLI**		Ambientale	Ambientale	Ambientale	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Umana	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Organizzativa	Organizzativa	Organizzativa	Organizzativa
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																											4	4	4	4
A.2	La politica di sicurezza è revisionata su base annuale																											4	4	4	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																											4,5	4,5	4,5	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																											4,5	4,5	4,5	4,5
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																											4,5	4,5	4,5	4,5
A.6	La politica di sicurezza è revisionata su base semestrale																											5	5	5	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					4	4	4	4	4					4	4	4											4	4	4	4
B.2	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	4	4												4	4	4
B.3	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			4,5	4,5	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			5	5	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	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															4	4	4
2	sicurezza per la				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

3	misure di sicurezza per				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	a membri del personale				5	5	5	5	5	5		5		5			5			5		5		5	5	5		5		5
D	**Gestione delle risorse**																														
1	dell'infrastruttura	4	4	4							4						4	4	4	4	4	4	4	4	4	4		4		4
2	oggetto di revisione e	4	4	4							4						4	4	4	4	4	4	4	4	4	4		4		4
3	misure di sicurezza e	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	oggetto di revisione e	5	5	5							5						5	5	5	5	5	5	5	5	5	5		5		5
E	**Cambio di gestione**																														
1	applicate per le							4	4	4			4	4			4	4	4	4	4	4	4	4	4	4		4		4
2	procedure per lo																														
3	regole per il cambio					5	5				5	5		5			5											5	5	5
F	**Responsabili del trattamento**																														
1	documentate linee guida					4									4	4											4	4	4	4
2	tempistiche di				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	accordo tra il titolare e il					4									4	4											4	4	4	4
4	verifica della conformità					3									3	3		3	3	3	3	3	3	3	3	3	3	3	3	3	3
5	accordi di					5									5	5		5	5	5	5	5	5	5	5	5	5	5	5	5	5
G	**Gestione degli incidenti / violazione dei dati pesonali**																														
1	di disaster recovery e di	3	3	3	3	3	3	3	3	3	3	3	3	3	3			3	3	3	3	3	3	3	3	3					
2	tecniche di alert per gli	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	documentato un piano	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	registrazione degli	5	5	5	5	5	5	5	5	5	5	5	5	5	5			5	5	5	5	5	5	5	5	5					5
H	**Business continuity**																														
1	sicurezza per garantire il	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
2	tecnico di business	3	3	3	3	3	3	3	3	3	3	3	3	3	3			3	3	3	3	3	3	3	3	3		3		3
3	misure per	3	3	3	3	3	3	3	3	3	3	3	3	3	3			3	3	3	3	3	3	3	3	3		3	3	3
4	personale specifico con	5	5	5	5	5	5	5	5	5	5	5	5	5	5			5	5	5	5	5	5	5	5	5	5	5	5	5
5	alternativa a seconda	5	5	5	5						5			5				5	5	5	5	5	5	5	5	5			5	
I	**Riservatezza del personale**																														
1	comunicazione dei ruoli,					4	4	4	4	4	4	4	4		4	4	4										4	4	4	4
2	dipendenti al rispetto					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
3	specifiche clausole di					5		5				5			5	5								5			5	5	5	5
J	**Formazione**																														
1	tecniche di informazione											4	4				4										4	4	4	4
2	programmi di					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
3	formazione con scopi e					5	5	5	5	5	5	5	5		5	5	5										5	5	5	5
K	**Controllo accessi e autenticazione**																														
1	controllo degli accessi,					4					4					4	4			4						4	4	4	4	4	4
2	sicurezza per					4	4					4				4	4							4			4	4	4	4	4
3	di autenticazione per				4	4								4				4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	sicurezza per impedire				4	4								4				4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	regole di composizione				4,5	4,5								4,5						4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5
6	custodia delle password				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
7	l'autenticazione a due				5	5								4				4	4	4	4	4	4	4	4	4	4	4	4	4	4
8	autenticazione del				5	5								5						5				5	5		5	5	5	5	5
L	**Registrazione e monitoraggio**																														
1	all'eventuale				4	4	4	4	4	4				4				4	4	4	4			4			4	4	4	4	4
2	di protezione dei file di					4			4	4				4										4	4			4		4
3	all'eventuale					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	procedure per l'integrità					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	alert per le					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
M	**Sicurezza server / database**																														
.1	di configurazione dei					4			4	4				4						4	4			4	4	4		4		4
.2	la minimizzazione dei															3				3				3			3	3		3
.3	soluzioni di crittografia				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	crittografia delle unità di				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	tecniche di				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
.6	di database che				5	5	5	5				5	5	5	5		5	5		5				5				5	5	5
N	**Sicurezza della postazione di lavoro**																														
1	sicurezza per impedire				4	4	4	4	4	4				4	4				4			4	4	4	4	4	4	4		4
2	strumenti antivirus,				4	4							4	4					4	4	4	4		4	4	4				4
3	non permettere agli												3	3				3	3	3	3	3	3	3	3	3	3	3		3
4	di sessione per				3	3					3	3		3						3	3	3	3	3				3	3	3
5	aggiornamenti di				4	4								4				4	4	4	4	4	4	4	4	4	4	4	4	4
6	frequenza nella				4,5													4,5	4,5	4,5	4,5	4,5		4,5	4,5	4,5				
7	misure tecniche per				3	3	3	3						3			3										3	3	3	3
8	misure per la restrizione												5	5	5												5	5	5	5
9	crittografia completa				5	5	5	5			5	5	5	5	5			5	5	5				5				5	5	5
O	**Sicurezza di rete / comunicazione**																														
1	crittografia tramite												4	4	4			4		4				4				4	4	4
2	regole per l'attivazione				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
3	misure per l'accesso				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	firewall e sistemi di				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	di blocco della				1	1	1	1			1	1	1	1	1			1	1	1	1	1	1	1	1	1	1	1		1
6	segregazione della rete				5	5	5	5			5	5	5	5	5			5	5	5	5	5	5	5	5	5	5	5		5
7	sistema IT mediante				1	1								1						1				1			1			
P	**Backup**																														
1	di backup e ripristino	4	4	4	4					4	4		4	4	4	4	4	4	4	4	4	4	4	4		4	4	4	4	4	4
2	custodia e di protezione	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	monitoraggio per la	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	nell'esecuzione dei	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	test dei supporti di	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
6	dei backup incrementali	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
7	di archiviazione delle	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
8	servizi di terze parti per	4,5	4,5	4,5	4,5					4,5	4,5		5	5	5	5	5	5	5	5	5	5	5	5		4,5	4,5	4,5	4,5	4,5	4,5
9	procedure di crittografia	5	5	5	5					5	5		5	5	5	5	5	5	5	5	5	5	5	5		5	5	5	5	5	5
Q	**Dispositivi mobili portatili**																														
1	sicurezza per l'accesso				4	4	4	4	4	4	4	4		4	4		4	4	4	4	4	4	4	4			4	4	4	4	
2	all'eventuale pre-				1	1	1	1	1	1	1	1		1	1		1	1	1	1	1	1	1	1			1	1	1	1	
3	i livelli di protezione dei					1	1	1				1	1	1	1												1	1	1	1	
4	di definizione di ruoli e					4,5	4,5	4,5				4,5	4,5	4,5	4,5												4,5	4,5	4,5	4,5	
5	misure per la												1				1										1	1	1	1	
6	misure per la												4,5				4,5										4,5	4,5	4,5	4,5	
7	misure per il caso di				4,5	4,5					4,5	4,5		4,5													4,5	4,5	4,5	4,5	
8	all'eventuale				3	3	3	3	3	3	3	3		3							3				3	3		3	3	3	3	
9	crittografia dei dati				3	3	3	3	3	3	3	3		3							3				3			3	3	3	3	
R	**Sicurezza del ciclo di vita delle applicazioni**																														
1	aggiornamento delle				4							4	4	4				4	4	4	4	4		4	4	4				4	
2	sicurezza specifici per le				4							4	4	4				4	4	4	4	4		4	4	4				4	
3	tecnologie e tecniche				4	4	4	4	4	4	4	4	4	4	4	4	4										4	4	4	4	
4	pratiche di codifica				3			3			3	3	3	3				3	3	3	3	3		3			3	3	3	3	
5	strumenti di convalida				3						3	3		3				3	3	3	3	3		3	3	3					
6	vulnerabilità e di					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	
7	certa frequenza ai test					3	3	3	3	3				3				3	3	3				3	3	3	3	3	3	3	
8	di ottenimento delle					3	3	3	3	3				3				3	3	3				3	3	3	3	3	3	3	
9	valutazioni delle patch					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	
S	**Cancellazione / eliminazione dei dati**																														
1	per la distruzione dei					4	4	4		4						4								4		4	4	4	4	4	
2	di distruzione dei					1	1	1		1						1											1	1	1	1	
3	sovrascrittura dei					1				1	1	1				1											1	1	1	1	
4	contratti di servizi regole					4,5				4,5	4,5	4,5				4,5											4,5	4,5	4,5	4,5	
5	smagnetizzazione					5				5	5	5				5											5	5	5	5	
6	distruzione di supporti o					5				5	5	5				5											5	5	5	5	
T	**Sicurezza fisica**																														
1	protezione del perimetro				4	4								4							4		4				4	4	4	4
2	identificazione del				4,5	4,5								4,5						4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5	
3	e monitoraggio degli				4,5	4,5								4,5						4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5	
4	rilevamento degli intrusi				4,5	4,5								4,5						4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5	
5	esistono barriere fisiche				4,5	4,5								4,5			4,5			4,5				4,5	4,5	4,5	4,5	4,5	4,5	4,5	
6	periodica delle aree																														
7	protezione contro	4,5	4,5	4,5										4,5	4,5						4,5	4,5	4,5			4,5					
8	limitate rispetto al				4,5	4,5								4,5							4,5	4,5	4,5	4,5			4,5	4,5	4,5	4,5	
9	protezione degli archivi				4,5	4,5								4,5			4,5							4,5			4,5	4,5	4,5	4,5	

MEDIA FINALE MITIGAZIONE PER MINACCIA	**####**	**4,239**	**4,239**	**####**	**####**	**3,927**	**####**	**####**	**4,000**	**####**	**4,010**	**4,065**	**4,042**	**####**	**####**	**4,214**	**4,054**	**4,009**	**####**	**####**	**####**	**####**	**####**	**####**	**####**	**3,936**	**4,044**	**####**	**4,063**

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

	Natura	Misura di Sicurezza	Check	Note
1	MISURA	Accesso ai locali ai soli autorizzati	SI	
2	MISURA	Misure Antincendio (estintori etc.)	SI	
3	MISURA	Misure Antiallagamento	SI	
4	MISURA	Sistema Antifurto	SI	
5	MISURA	Manutenzione degli impianti	SI	
6	MISURA	Gruppo di Continuità (UPS)	SI	
7	MISURA	Conservazione dati sotto chiave	SI	
8	MISURA	Videosorveglianza	SI	
9	MISURA	Test periodici sulle misure di sicurezza (penetration test, vulnerability assessment etc.)	SI	
10	MISURA	Misure di tracciabilità (log etc.)	SI	
11	MISURA	Partizionamento	SI	
12	MISURA	Antivirus	SI	
13	MISURA	Firewall	SI	
14	MISURA	Aggiornamento sistema informatico	SI	
15	MISURA	Pseudonimizzazione / Cifratura / Crittografia	SI	
16	MISURA	Anonimizzazione	SI	
17	MISURA	Piano di Disaster Recovery / Business Continuity	SI	
18	MISURA	Back-Up	SI	
19	MISURA	Definizione delle procedure tecniche di Back-up	SI	
20	MISURA	Individuazione dell'incaricato al Back-up	SI	
21	MISURA	Credenziali di Autenticazione (User + Password)	SI	
22	MISURA	Verifica doppio passaggio (two-step verification - verifica a due fattori)	SI	
23	MISURA	Politica di gestione degli accessi	SI	
24	MISURA	Controllo degli accessi logici	SI	
25	MISURA	Protocolli sicurezza web (https, TSL, SSL etc.)	SI	
26	MISURA	Nomina amministratore sistema	SI	
27	MISURA	Inventario tecnico-informatico	SI	
28	MISURA	Regolamento Sistema Privacy	SI	
29	MISURA	Contratto di responsabile art. 28 GDPR	SI	
30	MISURA	Valutazione delle garanzie di compliance privacy di responsabili, sub-responsabili e/o contitolari	SI	
31	MISURA	Policy di revisione periodica dei rapporti contrattuali con i fornitori	SI	
32	MISURA	Designazione Delegati trattamento art. 29 GDPR	SI	
33	MISURA	Designazione incaricati autorizzati art. 29 GDPR	SI	
34	MISURA	Formazione di una lista degli incaricati autorizzati per classi omogenne di incarico	SI	
35	MISURA	Formazione di una lista degli incaricati autorizzati su base individuale	SI	
36	MISURA	Referente Privacy interno	SI	
37	MISURA	Responsabile/Referente IT	SI	
38	MISURA	Nomina DPO	SI	
39	MISURA	Audit periodici	SI	
40	MISURA	Istruzioni al Personale	SI	
41	MISURA	Misure per l'archiviazione digitale	SI	
42	MISURA	Misure per l'archiviazione cartacea	SI	
43	MISURA	Formazione del Personale	SI	
44	MISURA	Informative / consensi con policy di revisione	SI	
45	MISURA	Disciplinare uso Strumenti IT	SI	
46	MISURA	Disciplinare uso strumenti Office (Google/Microsoft)	SI	
47	MISURA	Procedura Data Breach	SI	
48	MISURA	Procedure di resilienza dei sistemi di trattamento dopo un data breach	SI	
49	MISURA	Procedure per assicurare la riservatezza, l'integrità, la disponibilità dei dati (RID)	SI	
50	MISURA	Procedura di aggiornamento periodico dell'antivirus	SI	
51	MISURA	Definizione delle procedure organizzative di Back-up	SI	
52	MISURA	Procedura per l'affidamento delle credenziali agli incaricati	SI	
53	MISURA	Procedure di controllo sulle credenziali	SI	
54	MISURA	Politiche di privacy by design / by default	SI	
55	MISURA	Misure NIS2: si rinvia alla separata documentazione	SI	

#ID	Natura	SANITÀ: Misure di Sicurezza specifiche	Check	Note
56	MISURA	Accesso controllato ai locali di conservazione dei dati genetici	SI	
60	MISURA	Procedure per l'accesso agli archivi dei dati particolari	SI	
68	MISURA	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	SI	
70	MISURA	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	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.

...

#ID	Descrizione Minaccia	Natura Minaccia	Conseguenze	Mitigazione del Rischio	Probabilità residua	Impatto Residuo	Rischio residuo	Media 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	PARZIALMENTE	2	4	8,000	
7	Diffusione non autorizzata	Umana	R	PARZIALMENTE	2	4	8,000	
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	2	3	6,000	
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	3,448
16	Cessazione rapporto / turnover	Umana	RID	SI	1	1	1,000	
17	Attacco informatico	Tecnica	RID	SI	2	3	6,000	
18	Virus informatico	Tecnica	RID	SI	2	3	6,000	
19	Intromissione nel sistema	Tecnica	RID	SI	2	3	6,000	
20	Danno tecnico informatico	Tecnica	RID	SI	1	3	3,000	
21	Malfunzionamento informatico	Tecnica	RID	PARZIALMENTE	1	4	4,000	
22	Malfunzionamento tecnico	Tecnica	RID	PARZIALMENTE	1	3	3,000	
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	PARZIALMENTE	2	3	6,000	
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 ACCETTAT	BASSO

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 minaccia
Ambientale
Umana
Tecnica
Organizzativa

Nella presente scheda sono illustrati i rischi residui correlati alle possibili minacce, con indicazione della loro natura (Ambientale, Umana, Tecnica, Organizzativa) e delle 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 residuo è considerato all'esito dell'applicazione delle misure di mitigazione di cui ai protocolli e relative misure di sicurezza applicate, come illustrate nelle precedenti schede. Il grado di rischio residuo è calcolato sempre 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".
Il rischio è poi confrontato con quello che il titolare ritiene di poter accettare secondo la propria valutazione ed accountability.
Se il rischio è inferiore ad un grado elevato (alto), il titolare non richiede la consultazione preventiva del Garante ai sensi dell'art. 36 GDPR; laddove permanga elevato, in assenza di misure adottate dal titolare del trattamento per attenuare il rischio o in caso di loro inefficacia a ridurlo, viceversa viene richiesta la consultazione preventiva del Garante ai sensi dell'art. 36 GDPR.

#ID	Descrizione Minaccia	Natura Minaccia	Conseguenze	Considerata	Probabilità Originaria	Impatto Originario	Rischio Inerente (Originario)	Media Rischio Inerente		Mitigazione del Rischio	Probabilità residua	Impatto Residuo	Rischio residuo	Media Rischio Residuo
1	Incendio	Ambientale	ID	SI	2	4	8,000	12,931		SI	1	2	2,000	3,448
2	Allagamento	Ambientale	ID	SI	2	3	6,000			SI	1	1	1,000	
3	Crollo o altro fattore naturale/fisico	Ambientale	ID	SI	2	3	6,000			SI	1	1	1,000	
4	Furto di archivi o di singoli dati	Umana	RID	SI	3	5	15,000			SI	1	3	3,000	
5	Accesso non autorizzato	Umana	RI	SI	3	5	15,000			SI	1	3	3,000	
6	Comunicazione non autorizzata	Umana	R	SI	3	5	15,000			PARZIALMENTE	2	4	8,000	
7	Diffusione non autorizzata	Umana	R	SI	3	5	15,000			PARZIALMENTE	2	4	8,000	
8	Modifica dati non autorizzata	Umana	RID	SI	3	5	15,000			SI	1	3	3,000	
9	Distruzione dati non autorizzata	Umana	ID	SI	3	5	15,000			SI	1	3	3,000	
10	Perdita dati o dispositivo contenente da	Umana	RID	SI	3	4	12,000			SI	1	2	2,000	
11	Diffusione credenziali accesso	Umana	R	SI	3	5	15,000			SI	1	3	3,000	
12	Vittima di phishing o altra manipolazion	Umana	RID	SI	4	5	20,000			SI	2	3	6,000	
13	Altro trattamento illecito doloso	Umana	RID	SI	3	5	15,000			SI	1	3	3,000	
14	Altro trattamento illecito colposo	Umana	RID	SI	3	5	15,000			SI	1	3	3,000	
15	Mancata soddisfazione dei diritti	Umana	RID	SI	2	5	10,000			SI	1	3	3,000	
16	Cessazione rapporto / turnover	Umana	RID	SI	2	3	6,000			SI	1	1	1,000	
17	Attacco informatico	Tecnica	RID	SI	4	5	20,000			SI	2	3	6,000	
18	Virus informatico	Tecnica	RID	SI	4	5	20,000			SI	2	3	6,000	
19	Intromissione nel sistema	Tecnica	RID	SI	4	5	20,000			SI	2	3	6,000	
20	Danno tecnico informatico	Tecnica	RID	SI	2	5	10,000			SI	1	3	3,000	
21	Malfunzionamento informatico	Tecnica	RID	SI	2	5	10,000			PARZIALMENTE	1	4	4,000	
22	Malfunzionamento tecnico	Tecnica	RID	SI	2	4	8,000			PARZIALMENTE	1	3	3,000	
23	Altri fattori di divulgazione dati	Tecnica	R	SI	3	5	15,000			SI	1	3	3,000	
24	Altri fattori di corruzione dati	Tecnica	I	SI	3	5	15,000			SI	1	3	3,000	
25	Altri fattori di indisponibilità dei dati	Tecnica	D	SI	3	5	15,000			SI	1	3	3,000	
26	Mancata consapevolezza privacy	Organizzativa	RID	SI	3	4	12,000			PARZIALMENTE	2	3	6,000	
27	Inosservanza principi/adempimenti priv	Organizzativa	RID	SI	3	4	12,000			SI	1	2	2,000	
28	Carenza di personale/Turnover elevato	Organizzativa	RID	SI	2	3	6,000			SI	1	1	1,000	
29	Altre inefficienze organizzative	Organizzativa	RID	SI	3	3	9,000			SI	1	1	1,000	

Inerente si valuta l'applicazione dei corrispondenti Protocolli
in base al valore di Rischio Inerente si applicano le Misure di mitigazione

RISCHIO INERENTE (ORIG	ALTO	RISCHIO RESIDU	BASSO

Nella presente scheda è espressa la comparazione tra il rischio inerente (originario) ed il rischio residuo, una volta applicate le misure di mitigazione per effetto dell'implementazione dei protocolli di sicurezza e correlate misure di sicurezza.

RISCHIO ACCETTA	BASSO

egenda	
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 Minaccia
Ambientale
Umana
Tecnica
Organizzativa

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 RISCHIO MEDIO RISCHIO ALTO	1
N/A	RISCHIO BASSO RISCHIO MEDIO RISCHIO ALTO	neutro

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.