

**Valutazione di impatto  
Data Protection Impact Assessment  
(DPIA)**

Ente	<b>Azienda ULSS 3 Serenissima</b> Via Don Tosatto 147 30174 Mestre C.F. e P.I. 02798850273
------	---

Rappresentante legale	<b>Direttore Generale</b>
--------------------------	---------------------------

DPO	<b>Cervato Law &amp; Business s.r.l. Società tra Avvocati ref. Avv. Piergiovanni Cervato</b>
-----	--

Nome del trattamento	<b>Studio italiano, retrospettivo, osservazionale, multicentrico, volto a valutare l'efficacia e la sicurezza di loncastuximab tesirine in pazienti affetti da linfoma diffuso a grandi cellule B, ricaduto o refrattario, trattati in Italia con farmaco ad uso nominale (LONCOSS)</b>
-------------------------	---

Centro locale di Sperimentazione	<b>UOC Ematologia Ospedale dell'Angelo Mestre</b>
-------------------------------------	---

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, allorché 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



<b>Destinatari</b>		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.	---	---	---	---
<b>Periodo di conservazione</b>		10 anni	I dati contenuti nelle fonti, di cui sopra, seguono il ciclo di vita proprio definito dalla normativa di settore (massimario di scarto).	---	---	---	---	---	---
<b>Descrizione funzionale del trattamento</b>		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.							
<b>È stato nominato lo Sperimentatore Principale?</b>	<b>SI</b>	Lo sperimentatore principale nominato è il Dr. Maurizio Cavallari							
<b>Lo Sperimentatore Principale si avvale di un team ?</b>	<b>NO</b>	Lo sperimentatore principale non si avvale di un team							
<b>Come vengono reclutati gli interessati?</b>		In sede di visita per le persone vive che prestano il consenso.							
<b>Come vengono raccolti i dati (CRF)?</b>		tramite CRF							
<b>Come vengono selezionati i dati oggetto dello Studio (fonti)?</b>		cartelle cliniche dei pazienti							
<b>Come vengono pseudonimizzati i dati?</b>		ID univoco assistito							
<b>Come vengono anonimizzati i dati (se lo sono)?</b>		non applicabile							
<b>Come e dove vengono conservati i dati?</b>		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.							
<b>Come vengono elaborati i dati?</b>		Secondo il Protocollo di Studio							
<b>Quali risorse vengono utilizzate per lo Studio?</b>		Secondo il Protocollo di Studio							
<b>Come vengono comunicati i dati al Promotore?</b>		Scheda raccolta dati							
<b>I dati sono oggetto di pubblicazione scientifica?</b>	<b>SI</b>	Come da accordo tra Sponsor e Centro Sperimentale.							
<b>Il Comitato Etico si è espresso favorevolmente e con quali eventuali integrazioni?</b>	<b>SI</b>	Il Comitato Etico si è espresso favorevolmente sul Protocollo di Studio e relativa DPIA già predisposta dallo Sponsor.							
<b>Codici di condotta (se applicabile)</b>	<b>NO</b>	Non vi sono codici di condotta, ma standard applicabili (vedi sotto).							

<p><b>Standard o Linee Guida applicabili</b></p>	<p><b>SI</b></p>	<p>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."</p>	<p>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)</p>	<p>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]</p>	<p>Regolamento UE 536/2014 sui medicinali per uso umano, noto anche come "Regolamento Europeo sulle Sperimentazioni Cliniche"</p>	<p>Regolamento (UE) 2017/745 sui dispositivi medici (Medical Device Regulation, "MDR")</p>	<p>Regolamento (UE) 2017/746 sui dispositivi medici in vitro</p>	<p>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)</p>		
		<p>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</p>	<p>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</p>	<p>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</p>	<p>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"</p>	<p>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 regolativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto legislativo 14 maggio 2019, n. 52".</p>	<p>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)</p>	<p>Opinion 05/2014 on Anonymisation Techniques Adopted on 10 April 2014</p>		
<p><b>Sono stati consultati gli interessati e, se sì, in che modo e quale esito ha dato la consultazione?</b></p>	<p><b>NO</b></p>	<p>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.</p>								
<p><b>È stato consultato il DPO?</b></p>	<p><b>SI</b></p>	<p>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).</p>								

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 esplicito 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 diritti previsti dal Regolamento.	---	---	---
In applicazione delle disposizioni previste dal Garante per l'applicazione dell'art. 110 Codice Privacy, come si è tentato di contattare le persone coinvolte dallo Studio e quali sono i motivi che viceversa hanno reso impossibile tale contatto?		Il P.I. svolge i tentativi previsti (solitamente 3) e nei casi di impossibilità al contatto redige l'apposita dichiarazione sostitutiva del consenso. I tentativi sono costituiti da 1) verifica dell'esistenza in vita tramite anagrafe regionale / aziendale; 2) impiego dei recapiti telefonici in possesso nel centro ; 3) l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente.						
In applicazione dell'art. 110 Codice Privacy, la DPIA viene pubblicata e dove?	SI	La Dpia integrativa è disponibile nel sito web aziendale al seguente link <a href="https://trasparenza.aulss3.veneto.it/Sperimentazioni">https://trasparenza.aulss3.veneto.it/Sperimentazioni</a>						

<p><b>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)</b></p>	<p>SI</p>	<p>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;</p>	<p>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.</p>	<p>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).</p>	<p>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.</p>				
<p><b>I dati personali sono adeguati, pertinenti e limitati (minimizzazione dei dati) (art. 5, paragrafo 1, lett. c GDPR)?</b></p>	<p>SI</p>	<p>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.</p>						<p>Sono adottate tecniche di pseudonimizzazione / anonimizzazione necessarie alla conduzione dello Studio, secondo quanto previsto dal Protocollo.</p>	<p>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).</p>
<p><b>I dati sono esatti e aggiornati? (art. 5, paragrafo 1, lett. d GDPR)</b></p>	<p>SI</p>	<p>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.</p>							
<p><b>La conservazione è limitata (art. 5, par. 1, lett. e GDPR)?</b></p>	<p>SI</p>	<p>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</p>							
<p><b>Il trattamento garantisce integrità e riservatezza? (art. 5, par. 1, lett. f. GDPR)</b></p>	<p>SI</p>	<p>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.</p>							
<p><b>Il titolare dimostra il rispetto dei principi (accountability) (art. 5 par. 2 GDPR)?</b></p>	<p>SI</p>	<p>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 raccogliabile, al fine di invocare la base giuridica prevista dall'art. 110 Codice Privacy.</p>							
<p><b>Le informazioni sono fornite all'interessato e come (art. 12, 13 e 14 GDPR)?</b></p>	<p>SI</p>	<p>"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."</p>							
<p><b>È garantito il diritto di accesso e come può essere esercitato (art. 15 GDPR)?</b></p>	<p>SI</p>	<p>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.</p>							
<p><b>È garantito il il diritto di rettifica e/o integrazione e come può essere esercitato (art. 16 GDPR)?</b></p>	<p>SI</p>	<p>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.</p>							
<p><b>È garantito il diritto di cancellazione e come può essere esercitato (art. 17 GDPR)?</b></p>	<p>SI</p>	<p>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.</p>							

<b>È garantito il diritto di limitazione e come può essere esercitato (art. 18 GDPR)?</b>	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.
<b>È garantito il il diritto di portabilità e come può essere esercitato (art. 20 GDPR)?</b>	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.
<b>È garantito il diritto di opposizione e come può essere esercitato (art. 21 GDPR)?</b>	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.
<b>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)?</b>	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.  In 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.
<b>È garantito il diritto di revoca del consenso (art. 7 GDPR)?</b>	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.
<b>È garantito il diritto di reclamo (art. 77 GDPR)?</b>	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.
<b>Sono osservate le regole previste per il trattamento dei dati personali da parte dei responsabili per conto del titolare (art. 28 GDPR)?</b>	N/A	Il trattamento non prevede la nomina di responsabili del trattamento da parte del titolare
<b>Sono osservate le garanzie riguardanti trattamenti internazionali al di fuori dell'Unione Europea (capo V GDPR)?</b>	N/A	Il trattamento non prevede trasferimenti internazionali
<b>È attivata la consultazione preventiva del Garante (art. 36 GDPR)?</b>	N/A	La consultazione preventiva del Garante non è attivata in quanto non si rientra nei casi di cui all'art. 36 GDPR.

<b>Esito della valutazione di necessità e proporzionalità</b>	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)	<b>ALTO</b>
-------------------------------	-------------

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	

Cella: E1

Nota: =====

ID#AAAB2lhDpzs

(2026-03-27 09:45:36)

Flaggare se la minacca è stata considerata nell'analisi dei rischi. Se è N/A, inserire valore 1 sia come rischio che come impatto

#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
	<b>LIVELLO DEL PROTOCOLLO DA CONSIDERARE IN BASE AL RISCHIO INERENTE</b>	<b>ALTO</b>												
<b>A</b> <b>Politica di sicurezza e procedure per la protezione dei dati personali</b>														
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	4,417
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	
A.5	Esiste e si mantiene 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**



























#	MISURE	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	
		Incedio	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	Distribuzione dati non autorizzata	Perdita dati o dispositivi contenenti dati	Diffusione credenziali	Vittima di phishing o altra manipolazione	Altro trattamento illecito o doloso	Altro trattamento illecito o 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	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Tecnica	Organizzativa	Organizzativa	Organizzativa	Organizzativa
<b>A</b>																															
<b>A.1</b>																															
<b>A.2</b>																															
<b>A.3</b>																															
<b>A.4</b>																															
<b>A.5</b>																															
<b>A.6</b>																															
<b>B</b>																															
<b>B.1</b>																															
<b>B.2</b>																															
<b>B.3</b>																															
<b>B.4</b>																															
<b>B.5</b>																															
<b>C</b>																															
<b>C.1</b>																															
<b>C.2</b>																															

3	3	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	
4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
<b>D Gestione delle risorse</b>																										
1	1	4	4	4						4					4	4	4	4	4	4	4	4	4	4	4	
2	2	4	4	4						4					4	4	4	4	4	4	4	4	4	4	4	
3	3	4,5	4,5	4,5						4,5					4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	
4	4	5	5	5						5					5	5	5	5	5	5	5	5	5	5	5	
<b>E Cambio di gestione</b>																										
1	1							4	4	4					4	4									4	
2	2																									
3	3																									
<b>F Responsabili del trattamento</b>																										
1	1														4	4									4	
2	2														4	4									4	
3	3														4	4									4	
4	4														3	3									3	
5	5														5	5									5	
<b>G Gestione degli incidenti / violazione dei dati personali</b>																										
1	1	3	3	3	3	3	3	3	3	3	3	3	3	3												
2	2	4	4	4	4	4	4	4	4	4	4	4	4	4												4
3	3	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5	4,5												4
4	4	5	5	5	5	5	5	5	5	5	5	5	5	5												5
<b>H Business continuity</b>																										
1	1	4	4	4	4	4	4	4	4	4	4	4	4	4												4
2	2	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	3	3	3												3
4	4	5	5	5	5	5	5	5	5	5	5	5	5	5												5
5	5	5	5	5	5										5											5
<b>I Riservatezza del personale</b>																										
1	1														4	4	4									4
2	2														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	3														5	5										5
<b>J Formazione</b>																										
1	1														4	4										4
2	2														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	3														5	5	5	5	5	5	5	5	5	5	5	5
<b>K Controllo accessi e autenticazione</b>																										
1	1														4	4										4
2	2														4	4										4
3	3														4	4										4
4	4														4	4										4
5	5														4,5	4,5										4,5
6	6														4,5	4,5	4,5									4,5
7	7														5	5										5
8	8														5	5										5
<b>L Registrazione e monitoraggio</b>																										
1	1														4	4	4	4	4	4						4
2	2														4	4										4
3	3														4,5	4,5	4,5	4,5	4,5	4,5						4,5
4	4														4,5	4,5	4,5	4,5	4,5	4,5						4,5
5	5														4,5	4,5	4,5	4,5	4,5	4,5						4,5
<b>M Sicurezza server / database</b>																										
.1	.1														4	4										4
.2	.2																									3
.3	.3														4,5	4,5	4,5	4,5	4,5	4,5						4,5
.4	.4														4,5	4,5	4,5	4,5	4,5	4,5						4,5
.5	.5														4,5	4,5	4,5	4,5	4,5	4,5						4,5
.6	.6														5	5	5	5	5	5						5
<b>N Sicurezza della postazione di lavoro</b>																										
1	1														4	4										4
2	2														4	4										4
3	3														3	3										3
4	4														3	3										3
5	5														4	4										4
6	6														4,5	4,5	4,5	4,5	4,5	4,5						4,5
7	7														3	3	3	3	3	3						3
8	8														5	5	5									5
9	9														5	5	5	5	5	5						5
<b>O Sicurezza di rete / comunicazione</b>																										
1	1														4	4	4									4
2	2														4,5	4,5	4,5	4,5	4,5	4,5						4,5
3	3														4,5	4,5	4,5	4,5	4,5	4,5						4,5
4	4														4,5	4,5	4,5	4,5	4,5	4,5						4,5



#	Natura	Misura di Sicurezza	hec	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 omogenee 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	

#	Natura	SANITA: Misure di Sicurezza specifiche	hec	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	3,448
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	
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	Intrusione 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 ACCETTATO	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

<b>Natura minaccia</b>
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.

Cella: E1

Nota: =====

ID#AAAB2lhDpzc

(2026-03-27 09:45:36)

Flaggare se la minaccia è stata considerata nell'analisi dei rischi. Se è N/A, inserire valore 1 sia come rischio che come impatto

Cella: K1

Nota: =====

ID#AAAB2lhDpzw

(2026-03-27 09:45:36)

Flaggare se la minaccia è stata mitigata per effetto dell'applicazione dei Protocolli e delle Misure

#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 dati	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 manipolazione	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 privacy	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	

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

RISCHIO INERENTE (ORIGINARIO) **ALTO**

RISCHIO RESIDUO **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 ACCETTATO **BASSO**

legenda	
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

<b>Natura Minaccia</b>	
Ambientale	
Umana	
Tecnica	
Organizzativa	

Cella: E1

Nota: =====

ID#AAAB2lhDpzY

(2026-03-27 09:45:36)

Flaggare se la minaccia è stata considerata nell'analisi dei rischi. Se è N/A, inserire valore 1 sia come rischio che come impatto

Cella: K1

Nota: =====

ID#AAAB2lhDpzo

(2026-03-27 09:45:36)

Flaggare se la minaccia è stata mitigata per effetto dell'applicazione dei Protocolli e delle Misure

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

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

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

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

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

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

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

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

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